ON THE GROUP DEFINED FOR ANY GIVEN FIELD BY THE MULTIPLICATION TABLE OF ANY GIVEN FINITE GROUP*

BY

LEONARD EUGENE DICKSON

Introduction.

In two papers,† each having the title "On the Continuous Group that is defined by any given Group of Finite Order," BURNSIDE establishes certain results of decided interest and importance, among them being the theorems‡ of FROBENIUS on the irreducible factors of group-determinants. The object of this paper is the development of the theory of analogous groups in any arbitrary field or domain of rationality. In particular, when the field is the general Galois field of order p^n, we obtain a doubly-infinite system of finite groups corresponding to each given finite group. An exceptional case not treated here is that of a field having a modulus which is a factor of the order of the given finite group.§

BURNSIDE bases his work upon several theorems proved by means of the LIE theory of continuous groups. The corresponding theorems for an arbitrary field are here derived by simple rational processes (§§ 2, 3). The auxiliary theorems on invariant-factors (the "Elementartheiler" of WEIERSTRASS) are established in § 4 by means of the canonical form of a linear transformation in any field. The later developments (§§ 5–7) run parallel to the corresponding parts of BURNSIDE's treatment, but include essential modifications.

The results find application in the problem of the representation of a given finite group as a group of linear transformations in a given field upon the smallest number of variables. That the introduction of the concept of a field gives rise to a generalization of KLEIN's normal problem may be illustrated by the fact that a given group may be represented as a modular group upon a smaller number of variables than is possible for a representation as an algebraic linear group.

* Presented to the Society (Chicago) March 29, 1902. Received for publication March 14, 1902.

† Proceedings of the London Mathematical Society, vol. 29 (1898), pp. 207–224, 546–565.

‡ *Über die Primfactoren der Gruppendeterminante*, Berliner Sitzungsberichte, 1896, pp. 1343–1382.

§ In a paper to be presented to the London Mathematical Society, I propose to consider this case, at least for certain classes of groups, and to give additional examples of the general theory.

§1. *Definition of the group G.*

Let the operators of a given finite group g be s_1 (identity), $s_2, \cdots, s_n$. The (left-hand) multiplication table of the group is derived from the array

$$(1) \qquad \begin{array}{ccccccccc} s_1^{-1} & s_2^{-1} & \cdots & s_k^{-1} & \cdots & s_n^{-1} \\ s_2 s_1^{-1} & s_2 s_2^{-1} & \cdots & s_2 s_k^{-1} & \cdots & s_2 s_n^{-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ s_n s_1^{-1} & s_n s_2^{-1} & \cdots & s_n s_k^{-1} & \cdots & s_n s_n^{-1} \end{array}$$

by replacing each product by the equivalent operator of the group. We consider n arbitrary elements of the field F and assign to them the single-index notation x_{s_i} or x_i and also the double-index notations $x_{s_i s_j}$ or x_{ij}, $x_{s_i s_j^{-1}}$ or $x_{ij^{-1}}$, with the understanding that

$$(2) \qquad x_{ij} = x_k, \quad x_{ij^{-1}} = x_i \qquad (\text{if } s_i s_j = s_k, \text{ whence } s_i s_j^{-1} = s_i).$$

Consider the following matrix defined by the table (1):

$$(3) \qquad \begin{pmatrix} x_{11^{-1}} & x_{12^{-1}} & \cdots & x_{1k^{-1}} & \cdots & x_{1n^{-1}} \\ x_{21^{-1}} & x_{22^{-1}} & \cdots & x_{2k^{-1}} & \cdots & x_{2n^{-1}} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_{n1^{-1}} & x_{n2^{-1}} & \cdots & x_{nk^{-1}} & \cdots & x_{nn^{-1}} \end{pmatrix}.$$

Each variable x_i occurs once and but once in each row (or column). Hence any variable x_i occurs in exactly n places in the matrix. For all n places, the adjoint (first minor with proper sign) of x_i is the same.* In proof, denote by $A_{j,k}$ the adjoint of $x_{jk^{-1}}$. Consider first the adjoint

$$A_{j,j} \equiv |x_{ik^{-1}}| \qquad (i, k = 1, \cdots, j-1, j+1, \cdots, n).$$

Set $s_i = s_u s_j$, $s_k = s_v s_j$, so that $x_{ik^{-1}} = x_{uj^{-1}v^{-1}} = x_{uv^{-1}}$. Then

$$A_{j,j} = |x_{uv^{-1}}| \equiv A_{1,1} \qquad (u, v = 2, 3, \cdots, n).$$

To show next that $A_{j,k} = A_{c,1}$, where $c = jk^{-1}$, we set

$$x_{cit^{-1}} = x'_{it^{-1}} \qquad (i, t = 1, \cdots, n).$$

Since ci and i run simultaneously through the series of n operators,

$$\pm |x_{it^{-1}}| = |x_{cit^{-1}}| \equiv |x'_{it^{-1}}|.$$

* FROBENIUS, *Über Gruppencharaktere*, Berliner Sitzungsberichte, 1896, pp. 985–1021, § 6.

To obtain $x_{jk^{-1}} \equiv x_e$ in $|x_{cir^{-1}}|$, we must take $i = t$; the corresponding term of $|x'_{it^{-1}}|$ is therefore in the main diagonal. But $A'_{1,1} = A'_{2,2} = \cdots = A'_{n,n}$.

Consider the set of transformations, defined by the matrix (3),

$$X: \qquad \xi'_s = \sum_{i=1}^{n} x_{si^{-1}} \xi_i \qquad (s = 1, \cdots, n),$$

in which $x_1, \cdots, x_n$ take all sets of values in the field F such that $\Theta(x) \neq 0$, where $\Theta(x)$ denotes the determinant of the matrix (3). Then $\Theta(x)$ is called the *group-determinant of* g. In view of the preceding proof, the inverse of every such transformation X belongs to the set. Let

$$Y: \qquad \xi'_s = \sum_{i=1}^{n} y_{si^{-1}} \xi_i \qquad (s = 1, \cdots, n)$$

be a second transformation of the set. Then

$$y_{ij} \equiv y_k \qquad (\text{if } s_i s_j = s_k). \tag{2'}$$

Applying first X and then Y, we obtain the transformation

$$Z \equiv XY: \qquad \xi'_s = \sum_{i=1}^{n} z_{si^{-1}} \xi_i \qquad (s = 1, \cdots, n),$$

where

$$z_{si^{-1}} \equiv \sum_{j=1}^{n} y_{sj^{-1}} x_{ji^{-1}} \qquad (s, i = 1, \cdots, n). \tag{4}$$

In view of the properties (2) and (2'), it follows that *

$$z_{ij} = z_k \qquad (\text{if } s_i s_j = s_k). \tag{2''}$$

Hence the set of transformations X forms a group G.

§ 2. *Determination of the group G', reciprocal to G.*

Denote by X_k the particular transformation X given by the values

$$x_k = 1, \quad x_j = 0 \qquad (j = 1, \cdots, n; j \neq k).$$

Then $x_{si^{-1}}$ is zero unless $s_i = s_k^{-1} s_s$, so that we have

$$X_k: \qquad \xi'_s = \xi_{k^{-1}s} \qquad (s = 1, \cdots, n),$$

where $\xi_{k^{-1}s} \equiv \xi_i$ if $s_k^{-1} s_s = s_i$. If s_k is of period κ, the transformation X_k corresponds to a *regular* substitution X'_k on n letters, the general cycle being

$$(\xi_j \xi_{k^{-1}j} \xi_{k^{-2}j} \cdots \xi_{k^{-(\kappa-1)}j}).$$

* Hence relations (4) may be written in either of the forms:

$$s_i = \sum_{r=1}^{n} y_r x_{r^{-1}i}, \quad z_{st} = \sum_{r=1}^{n} y_r x_{ti}.$$

The regular substitution group composed of the substitutions $X_1', \cdots, X_n'$ is simply isomorphic with the group g in such a way that X_k' corresponds to s_k^{-1}.

Consider an arbitrary linear homogeneous transformation

$$\xi_i' = \sum_{j=1}^{n} a_{i,j}\xi_j \qquad (i=1, \cdots, n). \tag{5}$$

If $\sigma_1, \sigma_2, \cdots, \sigma_n$ form a permutation of $1, 2, \cdots, n$, the linear transformation

$$\xi_i' = \xi_{\sigma_i} \qquad (i=1, \cdots, n)$$

transforms (5) into the following transformation:

$$\xi_i' = \sum_{j=1}^{n} a_{\sigma_i, \sigma_j}\xi_j \qquad (i=1, \cdots, n).$$

The latter is identical with the transformation (5) if, and only if,

$$a_{i,j} = a_{\sigma_i, \sigma_j} \qquad (i, j=1, \cdots, n)$$

Hence the conditions that the n transformations X_k shall be commutative with the transformation (5) are

$$a_{i,j} = a_{k^{-1}i,\, k^{-1}j} \qquad (i, j, k=1, \cdots, n). \tag{6}$$

For $i = 1, \cdots, n$, we set $w_{i^{-1}} = a_{1,i}$, and set $w_{ab} = w_c$ if $s_a s_b = s_c$. Then by (6)

$$a_{i,j} = a_{1,\, i^{-1}j} = w_{j^{-1}i}.$$

Hence the transformation (5) may be written in the form

$$W: \qquad \xi_s' = \sum_{i=1}^{n} w_{i^{-1}s}\xi_i \qquad (s=1, \cdots, n).$$

Every transformation W is commutative with every transformation X. Indeed, the product XW replaces ξ_s by a linear function in which the coefficient of ξ_i is

$$\lambda_{si} \equiv \sum_{j=1}^{n} w_{j^{-1}s}x_{ji^{-1}}.$$

For s and i fixed, the operators s_j and $s_s s_j^{-1} s_i$ run simultaneously through the set of n operators of g. Replacing j by $sj^{-1}i$, we get

$$\lambda_{si} = \sum_{j=1}^{n} w_{i^{-1}j}x_{sj^{-1}}.$$

But this expression is the coefficient of ξ_i in the linear function by which the product WX replaces ξ_s.

It follows that the group G' of all the transformations W is the largest n-ary linear homogeneous group in the field F, each of whose transformations is commutative with every transformation X of G. Evidently the group G' may be defined by the right-hand multiplication table for the group g precisely as G was defined by its left-hand multiplication table. Hence G is the largest group of n-ary linear transformations in F which are commutative with every transformation of G'. Hence the groups G and G' are *reciprocal* to each other.

§ 3. *The commutative subgroup H.*

To obtain the transformations common to G and G', we must set

$$x_{si^{-1}} = w_{i^{-1}s} \qquad (i, s = 1, \cdots, n).$$

Setting $s_i^{-1} s_s = s_r$, so that $s_s s_i^{-1} = s_i s_r s_i^{-1}$, we get

$$x_{iri^{-1}} = w_r \qquad (i, r = 1, \cdots, n).$$

Hence the necessary and sufficient conditions that a transformation X of G shall belong to the group G' are that the variables $x_1, \cdots, x_n$ whose subscripts correspond to conjugate operators are all equal. Hence the transformations

$$E: \qquad \xi'_s = \sum_{i=1}^{n} e_{si^{-1}} \xi_i \qquad (s = 1, \cdots, n),$$

in which $e_1, \cdots, e_n$ run through every set of elements of F such that $e_j = e_k$ if s_j and s_k are conjugate in g and such that the determinant D_e of E is not zero, form a commutative group H. It is composed of all the self-conjugate transformations of G. This determinant D_e is called the *special group-determinant of g*. If r be the number of distinct sets of conjugate operators in g, exactly r of the e's are distinct and will be designated $\epsilon_1 = e_1, \epsilon_2, \cdots, \epsilon_r$. Since the inverse of the general transformation E belongs to the group H, the adjoint ϵ'_k of ϵ_k, in whatever position it occurs in D_e, is always the same. Let n_k denote the number of operators in the kth set of conjugates in the group g of order n. Then ϵ_k occurs exactly n_k times in each row of D_e, and altogether $n n_k$ times in the determinant. We derive therefore the *algebraic* identity

$$\epsilon'_k \equiv \frac{1}{n n_k} \frac{\partial D_e}{\partial \epsilon_k}. \tag{7}$$

The division of $\partial D_e / \partial \epsilon_k$ by $n n_k$ must first be performed if we are to apply (7) in the case of a field F having a modulus which divides n.

§ 4. *Invariant-factors of a linear transformation.*

By the *characteristic determinant* (with parameter ρ) of the transformation (5) is meant the determinant

$$D(\rho) \equiv \begin{vmatrix} a_{11}-\rho & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22}-\rho & a_{23} & \cdots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn}-\rho \end{vmatrix}.$$

Then $D(0)$ is the determinant of the transformation; it is assumed to be different from zero in the field F. The rth minors of $D(\rho)$ are polynomials in ρ with coefficients in F not all zero. The unique polynomial of highest degree in ρ which divides all of these minors and in which the coefficient of the highest power of ρ is $(-1)^n$ will be designated $D_r(\rho)$. It may be determined by EUCLID's algorithm for finding the greatest common divisor. Hence $D_r(\rho)$ has its coefficients in F. Now any $(r-1)$-th minor of $D(\rho)$ is the sum of certain rth minors each multiplied by an element of $D(\rho)$. Hence $D_r(\rho)$ divides $D_{r-1}(\rho)$ in the field F. The polynomials, with coefficients in F, defined by the quotients

$$\frac{D(\rho)}{D_1(\rho)}, \quad \frac{D_1(\rho)}{D_2(\rho)}, \quad \frac{D_2(\rho)}{D_3(\rho)}, \quad \cdots \tag{8}$$

are called the *invariant-factors* * of the characteristic determinant $D(\rho)$.

The importance of the invariant-factors is shown by the

THEOREM.—*The necessary and sufficient conditions that two n-ary linear homogeneous transformations A and A' with coefficients in F shall be conjugate within the n-ary linear homogeneous group in the field F are that the invariant-factors of the characteristic determinant of A shall be identical with the invariant-factors of that of A'.*

For the case in which F is the continuous field of all numbers, the theorem merely states the existence of a transformation T such that

$$T^{-1}AT = A',$$

without requiring that T shall belong to a *special* field. In this case, the theorem follows from a general result due to WEIERSTRASS. †

The proof that the conditions are necessary is very simple. If $T^{-1}AT = A'$, then the polynomials giving the expansions of the characteristic determinants of

* They are to be distinguished from the WEIERSTRASS "Elementartheiler," called the "einfachen Elementartheiler" by FROBENIUS, the latter being polynomials in ρ with coefficients involving the roots of $D(\rho) = 0$. But, if two determinants have the same "einfachen Elementartheiler," they have the same invariant-factors, and inversely.

† *Zur Theorie der bilinearen und quadratischen Formen*, *Werke*, II, pp. 19–44.

A and A' are identical. Let C and C' denote the unexpanded characteristic determinants of A and A' respectively. Any r-th minor of C' may be expressed as a sum of products of three factors, the first an r-th minor of $|T^{-1}|$, the second an r-th minor of C, the third an r-th minor of $|T|$. Let the coefficients of T belong to the field F. Then every common divisor of all the r-th minors of C is a divisor (with coefficients in F) of all the r-th minors of C'. Since $TA'T^{-1} = A$, the inverse is true. Hence $D_r(\rho) = D'_r(\rho)$.

To prove that the conditions are sufficient,* apply to A a linear transformation (not belonging to F, in general) to reduce it to its canonical form A_1:

$$(9)\qquad \begin{aligned} &\eta'_{i\alpha} = K_i\eta_{i\alpha}, \quad \eta'_{i\alpha} = K_i\eta_{i\alpha} + K_i\eta_{i\alpha-1} && (i=1,\cdots,k);\\ &\zeta'_{ib} = L_i\zeta_{ib}, \quad \zeta'_{i\beta} = L_i\zeta_{i\beta} + L_i\zeta_{i\beta-1} && (i=1,\cdots,i);\\ &\quad\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

in which the following notations have been employed.† Let

$$(-1)^n D(\rho) \equiv [F_k(\rho)]^\kappa [F_l(\rho)]^\lambda \cdots \qquad (n = k\kappa + l\lambda + \cdots),$$

$F_k(\rho), F_l(\rho), \cdots$ being distinct functions belonging to and irreducible in the field F, and having unity as coefficient of the highest power of ρ. The roots of $F_k(\rho) = 0$ are designated $K_1, \cdots, K_k$; the roots of $F_l(\rho) = 0$ are designated $L_1, \cdots, L_l$; etc. Then $\kappa, \lambda, \cdots$ are partitioned into positive integers

$$\kappa = a_1 + a_2 + \cdots + a_{r+1}, \quad \lambda = b_1 + b_2 + \cdots + b_{s+1}, \quad \cdots$$
$$(a_1 \geqq a_2 \geqq a_3 \cdots,\ b_1 \geqq b_2 \geqq b_3 \cdots,\ \cdots).$$

Then $a, b, \cdots$, denote integers selected arbitrarily from the respective sets

$$(a)\qquad 1,\ a_1+1,\ a_1+a_2+1,\ \cdots,\ a_1+a_2+\cdots+a_r+1;$$
$$(b)\qquad 1,\ b_1+1,\ b_1+b_2+1,\ \cdots,\ b_1+b_2+\cdots+b_r+1;$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Then α is any integer $\geqq \kappa$ and not an a; β is any integer $\geqq \lambda$ and not a b; and so on. Each η_{ij} is the same function of K_i that η_{1j} is of K_1. A similar statement may be made for the functions ζ_{ij} of L_i.

By the direct calculation of NETTO,‡ the invariant-factors of (9) are

$$\prod_{i=1}^{k}(\rho - K_i)^{a_1}\prod_{i=1}^{l}(\rho - L_i)^{b_1}\cdots, \quad \prod_{i=1}^{k}(\rho - K_i)^{a_2}\prod_{i=1}^{l}(\rho - L_i)^{b_2}\cdots, \ \cdots.$$

These invariant-factors may evidently be written in the simple form

$$(10)\quad [F_k(\rho)]^{a_1}[F_l(\rho)]^{b_1}\cdots, \ [F_k(\rho)]^{a_2}[F_l(\rho)]^{b_2}\cdots, \ [F_k(\rho)]^{a_3}[F_l(\rho)]^{b_3}\cdots, \ \cdots.$$

* The method of WEIERSTRASS does not seem adapted to prove the generalized theorem.

† Transactions, vol. 2 (1901), p. 393. The proof of the theorem quoted is given in the American Journal of Mathematics, vol. 24 (1902), pp. 101–108.

‡ *Zur Theorie der linearen Substitutionen*, Acta Mathematica, vol. 17 (1893), pp. 265–280

Upon expansion these expressions become polynomials in ρ with coefficients in F. But A_1 is the transform of A by a linear transformation. Hence the expressions (10) are the invariant-factors of the characteristic determinant of A. It follows that the canonical form is uniquely determined by the invariant-factors.

If, therefore, the invariant-factors of the characteristic determinants of A and A' are identical, A' is reducible to the same canonical form (9) as A. Hence, by the theorem concerning the canonical form, there exists a linear homogeneous transformation T on n variables with coefficients in F which transforms A into A'.

§ 5. *Factors of the special group-determinant D_e.*

Let A be one of the transformations E of the commutative group H and let B be a transformation such that $B^{-1}AB \equiv A_1$ is the canonical form (9) of A. Since $K_1, K_2, \cdots, K_k, L_1, \cdots, L_l, \cdots$ are all distinct, any transformation which is commutative with A_1 replaces each η_{ij} by a linear function of $\eta_{i1}, \cdots, \eta_{i\kappa}$ only, and replaces each ζ_{ij} by a linear function of $\zeta_{i1}, \cdots, \zeta_{i\lambda}$ only, etc. Hence every transformation of the commutative group $B^{-1}HB$ has these properties. Attending only to the variables $\eta_{i1}, \cdots, \eta_{i\kappa}$ (i being a fixed integer), we obtain a commutative group on κ variables. Unless the roots of the characteristic equation of each transformation of this group are all equal, we select one having at least two distinct roots and reduce it to its canonical form. Proceeding in this way, we obtain a transformation B_1 and a number of sets of variables such that every transformation of $B_1^{-1}HB_1$ replaces any variable of one set by a linear function of the variables of that set, thereby defining a partial group for each set; and such that the characteristic equation of every transformation of each partial group has all its roots equal.

Now the characteristic determinant $D_e(\rho)$ of the general transformation E of the group H is a homogeneous integral rational function of $\epsilon_1, \epsilon_2, \cdots, \epsilon_r, \rho$ of degree n. Also $D_e(\rho)$ is invariant under linear transformation. Hence $D_e(\rho)$ equals the product of the characteristic determinants of the partial transformations derived from E by the above process. Each of the latter determinants is therefore a homogeneous integral rational function of $\epsilon_1, \epsilon_2, \cdots, \epsilon_r, \rho$, and at the same time a power of a linear function of ρ. It is consequently a power of a linear homogeneous function of $\epsilon_1, \epsilon_2, \cdots, \epsilon_r, \rho$. Since $\epsilon_1 \equiv e_1$ occurs only in the combination $\epsilon_1 - \rho$, we may write

$$(11) \qquad (-1)^n D_e(\rho) = \prod_{i=1}^{s} (\rho - \epsilon_1 - a_{i2}\epsilon_2 - a_{i3}\epsilon_3 - \cdots - a_{ir}\epsilon_r)^{m_i} \quad \Big(\sum_{i=1}^{s} m_i = n\Big),$$

the s linear factors being distinct, each corresponding to a partial group. In case a factor f_1 involves quantities irrational with respect to F, the functions

conjugate to f_1 with respect to F must occur as factors in (11). Since $D_e(0) = D_e$, it follows that the special group-determinant of g decomposes into linear homogeneous functions of $\epsilon_1, \epsilon_2, \cdots, \epsilon_r$, a result due to FROBENIUS.

§ 6. *Canonical forms of the groups H and G.*

Consider the adjoints of the elements $\epsilon_1 - \rho, \epsilon_2, \cdots, \epsilon_r$ in the determinant $D_e(\rho)$. In view of (7), the k-th adjoint is identical, aside from the factor $1/nn_k$, with the partial derivative of $D_e(\rho)$ with respect to ϵ_k. Suppose that, in case the field F has a modulus p, the latter divides none of the numbers * $n, m_1, \cdots, m_s$. Then

$$\rho - \epsilon_1 - a_{i2}\epsilon_2 - \cdots - a_{ir}\epsilon_r \equiv \rho - \tau_i,$$

which occurs in $D_e(\rho)$ exactly to the power m_i, occurs exactly to the power $m_i - 1$ in the factor of highest degree in ρ which divides all the first minors of $D_e(\rho)$. Hence the first invariant-factor of $D_e(\rho)$ is $(\rho - \tau_1)\cdots(\rho - \tau_s)$. Since the characteristic determinant of the i-th partial group H_i is $(\tau_i - \rho)^{m_i}$, and its first invariant-factor in the field $F(\tau_i)$ is $\rho - \tau_i$, it follows that each invariant-factor is $\rho - \tau_i$. Indeed, each is of degree $\geqq 1$ and their product is of degree m_i. Hence the canonical form of the general transformation of H_i is

$$\xi'_{ij} = \tau_i \xi_{ij} \qquad (j = 1, \cdots, m_i). \tag{12}$$

Let a particular transformation, for which τ_i has the value τ'_i, be reduced to its canonical form of type (12). Without altering the latter, a second particular transformation, for which $\tau_i = \tau''_i$, can be reduced to its canonical form of type (12). Proceeding thus, we find that all the transformations of H_i can be reduced simultaneously to the form (12). Hence there exists a linear transformation which transforms the group H into the group H of the transformations

$$\xi'_{ij} = \tau_i \xi_{ij} \qquad (j = 1, \cdots, m_i;\ i = 1, \cdots, s). \tag{13}$$

If τ_1, for example, does not belong to the field F, its conjugates $\tau_1, \tau_2, \cdots, \tau_l$, with respect to F, must occur as multipliers in (13). By the canonical form theory, each ξ_{1j} is a linear function of the initial indices with coefficients involving only the elements of F and the irrationalities occurring in τ_1, while

$$\xi_{1j}, \quad \xi_{2j}, \quad \cdots, \quad \xi_{lj}$$

are conjugate with respect to F. Among the s multipliers τ_i, exactly r are in-

* Since $m_1, \cdots, m_s$ are divisors of n (FROBENIUS), only divisors p of n are excluded.

dependent with respect to F. It is shown later that $s = r$, so that the distinct multipliers τ_i in (11) are all independent.*

Let the groups G, G' become Γ, Γ' when expressed in terms of the new variables ξ_{ij}. Since every transformation of Γ (or Γ') is commutative with every transformation of H, every transformation of Γ (or Γ') must replace ξ_{ij} by a function of $\xi_{i1}, \cdots, \xi_{im_i}$ only. Let Γ_i and Γ_i' denote the partial groups on the latter variables. Every transformation of Γ_i is commutative with every one of Γ_i'. Since G (or G') involves linearly and homogeneously n parameters which are independent in F, Γ_i (or Γ_i') must involve linearly and homogeneously m_i parameters which are independent with respect to F. In fact, G is simply transitive in its n variables, so that Γ contains a transformation which replaces any given set of values of ξ_{ij} obeying the prescribed conjugacies with respect to F by any second set of values ξ_{ij} obeying the same conjugacies. Hence the general transformation of Γ_i may be written

$$\xi_{ij}' = \sum_{l,k}^{1,\cdots,m_i} a_{jkl}\tau_{ik}\xi_{il} \qquad (j = 1, \cdots, m_i), \tag{14}$$

where $\tau_{i1}, \cdots, \tau_{im_i}$ are linear functions of the n parameters of G, the functions being independent with respect to F. Moreover, the n parameters

$$\tau_{ik} \qquad (k = 1, \cdots, m_i;\ i = 1, \cdots, s)$$

are independent with respect to F, since otherwise the group in its initial form G would depend upon less than n independent parameters of F. Hence each partial group Γ_i is a subgroup of Γ.

Likewise Γ' contains as a subgroup the partial group Γ_i', whose transformations are of type (14), the variables ξ_{ij} being the same as before. Since every transformation (13), in which τ_i has for the coefficients of the irrationalities entering $\xi_{i1}, \cdots, \xi_{im_i}$ *arbitrary* elements in F, is commutative with every transformation of Γ', and leads to a transformation on the initial variables having its coefficients in F, it belongs to the group Γ (see end of § 2). Hence the self conjugate transformations of Γ form a group with s parameters independent with respect to F. By § 3 this number is r. Hence $s = r$.

§ 7. *Structure of G. Properties of the group-determinant.*

The group Γ is the direct product of the groups $\Gamma_1, \Gamma_2, \cdots, \Gamma_r$ which affect different variables. If τ_1 does not belong to F, the complete set of conjugates $\tau_1, \tau_2, \cdots, \tau_l$, with respect to F, defines a larger field F_l. To the latter belong the coefficients of the groups $\Gamma_1, \Gamma_2, \cdots, \Gamma_l$, which may be said to be

* This seems to be assumed by BURNSIDE (l. c., p. 557) in showing at this point that $s = r$.

conjugate with respect to the field F; their direct product is simply isomorphic with a group J_1 on m_1 variables and involving m_1 arbitrary parameters of F_{l_1}. By a suitable choice of notation, we may therefore express Γ as the direct product of certain groups $J_1, J_2, \cdots, J_\rho$ on different variables, J_i being a group on m_i variables and involving m_i arbitrary parameters of a field F_{l_i}, so that

$$m_1 l_1 + m_2 l_2 + \cdots + m_\rho l_\rho = n, \quad l_1 + l_2 + \cdots + l_\rho = r.$$

From the transformations (14) of the group J_i, we form the determinant

$$D_{\xi_i} \equiv \left| \sum_{l=1}^{m_i} a_{jkl} \xi_{il} \right| \qquad (j, k = 1, \cdots, m_i). \tag{15}$$

It is (relatively) invariant under every transformation W of the group J_i and hence is absolutely invariant under every transformation $W_1^{-1} W_2^{-1} W_1 W_2$ of the commutator group of J_i. A like result holds for every factor of D_{ξ_i} belonging to and irreducible in the field F_{l_i} (compare BURNSIDE, l. c., § 3, pp. 549, 550). Hence these irreducible factors are all invariants of the commutator group of Γ. Now the commutator group of G is the quotient-group of G by the subgroup H and hence is a group on n variables with $n - r$ parameters in F, and consequently has at most r independent invariants in F. Consider the $r = l_1 + l_2 + \cdots + l_\rho$ groups $J_1, \cdots, J_\rho$ and their conjugates with respect to F. Their determinants give r independent invariants of Γ and hence give rise to r independent functions in F which are invariants of G. Hence, for each value of i, the determinant (15) must be a power of an irreducible factor in F_{l_i}. The self-conjugate transformations of J_i form a group with one arbitrary parameter in F_{l_i}. It follows that the irreducible factor of (15) is linear only when $m_i = 1$ (compare BURNSIDE,* l. c., § 5). For $m_i > 1$, it must be a perfect square, $m_i = \mu_i^2$, and J_i is simply isomorphic with a linear homogeneous group on μ_i variables with coefficients in F_{l_i} (compare BURNSIDE, l. c., § 6). Since it involves μ_i^2 independent parameters, this group must be the general linear homogeneous group in F_{l_i} on μ_i variables. The transformations of J_i may therefore be given the form

$$z'_{tj} = u_{j1} z_{t1} + u_{j2} z_{t2} + \cdots + u_{j\mu_i} z_{t\mu_i} \qquad (t, j = 1, 2, \cdots, \mu_i),$$

the number of parameters u_{jk} being μ_i^2. The determinant corresponding to (15) is therefore the power μ_i of the determinant

$$|z_{tk}| \qquad (t, k = 1, 2, \cdots, \mu_i). \tag{16}$$

We may therefore state the following

THEOREM.—*Excluding the case in which the given field F has a modulus which divides the order n of the given finite group g, let the r linear factors*

* In a note offered to the Bulletin, I correct an error made by BURNSIDE in § 5.

of the special group-determinant be separated into sets of conjugates with respect to F, the sets containing $l_1, l_2, \cdots, l_\rho$ factors, respectively. Denote by $F_{l_1}, F_{l_2}, \cdots, F_{l_\rho}$ the respective enlarged fields. The group G defined in F by the multiplication table of g is the direct product of ρ groups simply isomorphic with the general linear homogeneous groups in the fields $F_{l_1}, F_{l_2}, \cdots, F_{l_\rho}$ on $\mu_1 = 1, \mu_2, \cdots, \mu_\rho$ variables, respectively, where $l_1\mu_1^2 + l_2\mu_2^2 + \cdots + l_\rho\mu_\rho^2 = n$. For each $i = 1, \cdots, \rho$, the general group-determinant contains l_i distinct factors of degree μ_i belonging to and irreducible in the field F_{l_i}, and conjugate with respect to F; each of these factors occurs exactly to the power μ_i in the group-determinant. The general factor may be expressed as a determinant (16) on μ_i^2 independent linear functions of the n elements of the group-matrix.

§ 8. *Two illustrative examples.*

Consider first the symmetric group g_6 on three letters, with the substitutions

$$s_1 = \text{identity}, \quad s_2 = (132), \quad s_3 = (123), \quad s_4 = (12), \quad s_5 = (13), \quad s_6 = (23).$$

Denote by X, T and C the respective matrices *

$$\begin{bmatrix} x_1 & x_3 & x_2 & x_4 & x_5 & x_6 \\ x_2 & x_1 & x_3 & x_5 & x_6 & x_4 \\ x_3 & x_2 & x_1 & x_6 & x_4 & x_5 \\ x_4 & x_5 & x_6 & x_1 & x_3 & x_2 \\ x_5 & x_6 & x_4 & x_2 & x_1 & x_3 \\ x_6 & x_4 & x_5 & x_3 & x_2 & x_1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -2 & 2 & -1 & -1 \\ -2 & 1 & 1 & -1 & 2 & -1 \\ 1 & -2 & 1 & -1 & 2 & -1 \\ 1 & 1 & -2 & -1 & -1 & 2 \end{bmatrix}, \quad \begin{bmatrix} \lambda & 0 & 0 & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 & 0 & 0 \\ 0 & 0 & a & b & 0 & 0 \\ 0 & 0 & d & c & 0 & 0 \\ 0 & 0 & 0 & 0 & a & b \\ 0 & 0 & 0 & 0 & d & c \end{bmatrix}.$$

The first matrix X is the group-matrix of g_6. The determinant of the second matrix T equals -2.3^5. If the field F has a modulus p, we assume that $p > 3$. Then † T defines a transformation which transforms that defined by X into that defined by C, where

$$\lambda = x_1 + x_2 + x_3 + x_4 + x_5 + x_6, \quad a = x_1 - x_2 + x_5 - x_6, \quad b = x_3 - x_2 + x_5 - x_4,$$
$$\mu = x_1 + x_2 + x_3 - x_4 - x_5 - x_6, \quad c = x_1 - x_3 - x_5 + x_6, \quad d = x_2 - x_3 + x_6 - x_4.$$

* For a simple and natural determination of the matrix T, from which follows incidentally the evaluation of its determinant, see the final reference in the introduction. For the case of a field containing an imaginary cube root of unity, DEDEKIND found a transformation having the desired property (Berliner Sitzungsberichte, 1897, p. 1007).

† Between the *matrices* the following relations therefore hold:

$$TXT^{-1} = C, \quad TX = CT.$$

Now λ, μ, a, b, c, d are independent functions of $x_1, \cdots, x_6$. Hence the group G of the transformations (x_i) is simply isomorphic with a group which is the direct product of two general unary linear groups in F and a general binary linear group in F.

The second example was chosen to illustrate the theory when the factors of the special group-determinant involve irrationalities. Aside from the cyclic groups, the dihedron group of order 10 is the simplest case in which irrationalities enter. A more difficult example is the simple group of order 60, the irrationality being $\sqrt{5}$. But no irrationality enters for a symmetric group (FROBENIUS).

The dihedron group g_{10} is generated by operators α, β such that

$$\alpha^5 = I, \quad \beta^2 = I, \quad \alpha\beta = \beta\alpha^{-1}.$$

Its operators fall into four distinct sets of conjugate operators:

$$I; \quad \alpha, \quad \alpha^4; \quad \alpha^2, \quad \alpha^3; \quad \beta, \quad \beta\alpha, \quad \beta\alpha^2, \quad \beta\alpha^3, \quad \beta\alpha^4.$$

Denote α^i by a_i and $\beta\alpha^i$ by β_i for $i = 1, 2, 3, 4$. The group-matrix is

$$\left(\begin{array}{c|c} A & B \\ \hline B & A \end{array}\right), \tag{17}$$

where

$$A \equiv \begin{Vmatrix} I & a_1 & a_2 & a_3 & a_4 \\ a_4 & I & a_1 & a_2 & a_3 \\ a_3 & a_4 & I & a_1 & a_2 \\ a_2 & a_3 & a_4 & I & a_1 \\ a_1 & a_2 & a_3 & a_4 & I \end{Vmatrix}, \qquad B \equiv \begin{Vmatrix} \beta & \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta \\ \beta_2 & \beta_3 & \beta_4 & \beta & \beta_1 \\ \beta_3 & \beta_4 & \beta & \beta_1 & \beta_2 \\ \beta_4 & \beta & \beta_1 & \beta_2 & \beta_3 \end{Vmatrix}.$$

By inspection, the group-determinant D is seen to have the factors

$$\delta \equiv I + a_1 + a_2 + a_3 + a_4 + \beta + \beta_1 + \beta_2 + \beta_3 + \beta_4,$$

$$\delta_1 \equiv I + a_1 + a_2 + a_3 + a_4 - \beta - \beta_1 - \beta_2 - \beta_3 - \beta_4.$$

If the field F has a modulus p, we assume that $p \neq 2, p \neq 5$. The transformation

$$\xi_1' = \sum_{j=1}^{10} \xi_j, \quad \xi_2' = \sum_{j=1}^{5} \xi_j - \sum_{j=6}^{10} \xi_j, \quad \xi_i' = \xi_i - \xi_1 \ (i = 3, 4, \cdots, 10)$$

has determinant 10. It transforms (17) into a matrix * having as first two rows

$$\begin{matrix} \delta & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \delta_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix}$$

and having zero as every element of the first column except that in the first row. New zero elements are introduced by transforming in succession by

$$[3,6],\quad [5,8],\quad [7,4],\quad [4,9],\quad [10,5],\quad [10,8],\quad [8,3],$$

where $[i,j]$ is a transformation affecting only ξ_i which it replaces by $\xi_i - \xi_j$. The resulting matrix has zeros at the intersections of the third, fifth, seventh, ninth rows [columns] with the fourth, sixth, eighth, tenth columns [rows]. Applying next the transformation

$$[10,8]^{-1}[4,6][6,10]\,(\xi_4' = \xi_8,\ \xi_8' = \xi_{10},\ \xi_{10}' = \xi_4,\ \xi_6' = -\xi_6),$$

we obtain a matrix in which the partial matrix on the variables $\xi_4, \xi_6, \xi_8, \xi_{10}$ is identical with that on $\xi_3, \xi_5, \xi_7, \xi_9$, viz., matrix M below. To make the elements of the second column, which lie in the third, $\cdots$, tenth rows, all zero, it suffices to transform by

$$\xi_3' = \xi_3 - \tfrac{1}{5}\xi_2,\quad \xi_5' = \xi_5 - \tfrac{1}{5}\xi_2,\quad \xi_7' = \xi_7 + \tfrac{1}{5}\xi_2,\quad \xi_9' = \xi_9 + \tfrac{1}{5}\xi_2,$$
$$\xi_4' = \xi_4 + \tfrac{2}{5}\xi_2,\quad \xi_6' = \xi_6 + \tfrac{2}{5}\xi_2,\quad \xi_8' = \xi_8 + \tfrac{3}{5}\xi_2,\quad \xi_{10}' = \xi_{10} - \tfrac{2}{5}\xi_2.$$

Transforming by $(\xi_4\xi_5\xi_7)(\xi_6\xi_9\xi_8)$, we obtain the final matrix

$$\left[\begin{array}{c|c|c} \begin{matrix}\delta & 0\\ 0 & \delta_1\end{matrix} & O & O \\ \hline O & M & O \\ \hline O & O & M \end{array}\right],$$

where each O denotes a matrix all of whose elements are zero, while M is the matrix

$$\left[\begin{matrix} I-a_4+\beta_1-\beta_2 & a_2-a_4+\beta_1-\beta_4 & -a_1+a_4-\beta_1+\beta_3 & -a_3+a_4+\beta-\beta_1 \\ -a_2+a_3+\beta_3-\beta_4 & I-a_2-\beta_1+\beta_3 & a_2-a_4+\beta-\beta_3 & -a_1+a_2+\beta_2-\beta_3 \\ a_3-a_4-\beta_2+\beta_3 & -a_1+a_3+\beta-\beta_2 & I-a_3+\beta_2-\beta_4 & a_2-a_3-\beta_1+\beta_2 \\ a_1-a_2+\beta-\beta_4 & a_1-a_4+\beta_2-\beta_4 & -a_1+a_3-\beta_1+\beta_4 & I-a_1-\beta_3+\beta_4 \end{matrix}\right].$$

* In this example, a matrix denotes the transformation defined by the matrix.

For a canonical form of still simpler type, we must resort to a transformation involving the irrationality $\sqrt{5}$. To obtain the special group-determinant, we must set $a_1 = a_4$, $a_2 = a_3$, $\beta = \beta_1 = \beta_2 = \beta_3 = \beta_4$. Then M becomes

$$M' \equiv \begin{vmatrix} I - a_1 & a_2 - a_1 & 0 & a_1 - a_2 \\ 0 & I - a_2 & a_2 - a_1 & a_2 - a_1 \\ a_2 - a_1 & a_2 - a_1 & I - a_2 & 0 \\ a_1 - a_2 & 0 & a_2 - a_1 & I - a_1 \end{vmatrix}.$$

Now M' may be transformed into the canonical form M'', in which the first two variables are multiplied by $I + a_1 y_2 + a_2 y_1$ and the last two by $I + a_1 y_1 + a_2 y_2$, where $y_1 = \frac{1}{2}(\sqrt{5} - 1)$, $y_2 = \frac{1}{2}(-\sqrt{5} - 1)$ are the roots of $y^2 + y - 1 = 0$. A transformation T such that $T^{-1} M' T = M''$ is given by the first of the following matrices, T^{-1} by the second:

$$\begin{vmatrix} 1 & \frac{-y_2}{\sqrt{5}} & y_1 - \frac{1}{\sqrt{5}} & \frac{-1}{\sqrt{5}} \\ 0 & y_1 & 1 & 1 \\ 1 & \frac{y_1}{\sqrt{5}} & y_2 + \frac{1}{\sqrt{5}} & \frac{1}{\sqrt{5}} \\ 0 & y_2 & 1 & 1 \end{vmatrix}, \quad \begin{vmatrix} \frac{-y_2}{\sqrt{5}} & \frac{-y_1}{5} & \frac{y_1}{\sqrt{5}} & \frac{y_1}{5} \\ 0 & \frac{1}{\sqrt{5}} & 0 & \frac{-1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{1}{5} & \frac{-1}{\sqrt{5}} & \frac{-1}{5} \\ \frac{-1}{\sqrt{5}} & \frac{3+\sqrt{5}}{10} & \frac{1}{\sqrt{5}} & \frac{-3-\sqrt{5}}{10} \end{vmatrix}.$$

It follows from the conjugacy of the variables in T and from the commutativity of M and M' that $T^{-1} M T$ has the form

$$M_1 \equiv \begin{vmatrix} A & B & 0 & 0 \\ C & D & 0 & 0 \\ 0 & 0 & A_1 & B_1 \\ 0 & 0 & C_1 & D_1 \end{vmatrix},$$

where A and A_1 are of the respective forms $a + a'\sqrt{5}$ and $a - a'\sqrt{5}$, etc. That M_1 is of the specified form is also shown by direct computation; then

$$A = I - \tfrac{1}{5}\sqrt{5}\,a_1 - \tfrac{1}{5}(y_2+3)a_2 + \tfrac{2}{5}\sqrt{5}\,a_3 + \tfrac{1}{5}\sqrt{5}(y_2-1)a_4 - \tfrac{1}{5}\sqrt{5}\,\beta + \beta_1 - \tfrac{1}{10}(5+3\sqrt{5})\beta_2 + \tfrac{2}{5}\sqrt{5}\,\beta_3 - \tfrac{1}{5}\sqrt{5}\,y_1\beta_4,$$

$$B = -\tfrac{1}{10}(7-\sqrt{5})(a_1-a_4) + \tfrac{1}{10}(1+3\sqrt{5})(a_2-a_3) + \tfrac{4}{5}\beta - \tfrac{1}{10}(5+\sqrt{5})\beta_1 + \tfrac{3}{10}(\sqrt{5}-1)\beta_2 + \tfrac{1}{10}(\sqrt{5}-1)\beta_3 + \tfrac{1}{10}(1-3\sqrt{5})\beta_4,$$

$$C = y_2(a_2+\beta_4-a_3-\beta_3) + a_1 + \beta - a_4 - \beta_2,$$

$$D = I + \tfrac{2}{5}\sqrt{5}\,a_2 + \tfrac{1}{10}(\sqrt{5}-5)a_3 - \tfrac{1}{5}\sqrt{5}\,a_4 - \tfrac{1}{10}(5+3\sqrt{5})(a_1-\beta_2) + \tfrac{1}{5}\sqrt{5}\,\beta - \beta_1 - \tfrac{2}{5}\sqrt{5}\,\beta_3 + \tfrac{1}{10}(5-\sqrt{5})\beta_4$$

For the determinant $\Delta \equiv AD - BC$ we obtain the value*

$$\begin{aligned} &I^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 - \beta^2 - \beta_1^2 - \beta_2^2 - \beta_3^2 - \beta_4^2 \\ &+ y_1(Ia_2 + Ia_3 + a_1a_3 + a_1a_4 + a_2a_4) \\ &+ y_2(Ia_1 + Ia_4 + a_1a_2 + a_2a_3 + a_3a_4) \\ &- y_1(\beta\beta_2 + \beta_1\beta_3 + \beta_2\beta_4 + \beta_3\beta + \beta_4\beta_1) \\ &- y_2(\beta\beta_1 + \beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_4 + \beta_4\beta). \end{aligned}$$

The value of $A_1D_1 - B_1C_1$ is obtained from Δ by interchanging y_1 with y_2.

That δ, δ_1, A, B, C, D, A_1, B_1, C_1, D_1 are independent functions of $I, a_1, \cdots, \beta_4$ follows from the fact that the final canonical form may be transformed into the initial matrix (17), so that $I, a_1, \cdots, \beta_4$ are linear functions of $\delta, \delta_1, \cdots, D_1$. To give a direct proof, we note that from δ and δ_1 may be derived

$$I + a_1 + a_2 + a_3 + a_4, \quad \beta + \beta_1 + \beta_2 + \beta_3 + \beta_4;$$

from C and C_1 may be derived $a_2 + \beta_4 - a_3 - \beta_3$, $a_1 + \beta - a_4 - \beta_2$; also

$$A + A_1 = 2I - a_2 - 3a_4 + 2\beta_1 - \beta_2 - \beta_4,$$

$$\sqrt{5}(A_1 - A_2) = -2a_1 + a_2 + 4a_3 - 3a_4 - 2\beta - 3\beta_2 + 4\beta_3 + \beta_4.$$

* This result was also computed directly by FROBENIUS's method. The characteristics of g_{10} are given by the table

f	χ_I	χ_{a_1}	χ_{a_2}	χ_β
1	1	1	1	1
1	1	1	1	−1
2	2	y_1	y_2	0
2	2	y_2	y_1	0

From these and the analogous expressions for $B \pm B_1$, $D \pm D_1$, we may derive $I, \alpha_1, \cdots, \beta_4$.

If $\sqrt{5}$ belongs to the field F, the group G defined by the matrix (17) is simply isomorphic with a group given by the direct product of the two general unary groups and two general binary groups, all belonging to F. If $\sqrt{5}$ serves to extend F to a larger field F_2, G is simply isomorphic with a group given by the direct product of two general unary groups in F (having the respective multipliers δ, δ_1) and a general binary group in F_2, viz.,

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

THE UNIVERSITY OF CHICAGO,
March 10, 1902.

NACHTRAG ZUM ARTIKEL: „ZUR ERKLÄRUNG DER BOGENLÄNGE U. S. W." (DIESES BANDES, S. 23 F.)*

VON

O. STOLZ

Den Lesern dieses Aufsatzes dürfte es nicht unwillkommen sein, wenn ich meine Darstellung der Lehre von der Rectification der Curven mit C. JORDAN's Darstellung derselben † vergleiche.

JORDAN geht von der nämlichen Erklärung der Länge des Bogens

$$x = \phi(t), \quad y = \psi(t) \qquad (\alpha \leqq t \leqq \beta), \tag{1}$$

aus, wie ich S. 26. Dann bemerkt er zunächst, dass, wenn die Summe

$$\sum_{r=1}^{n} |A_{r-1} A_r|, \tag{2}$$

bei $\lim \delta_r = 0\,(r = 1, \cdots, n)$ überhaupt einen endlichen Grenzwerth L hat, dieser *die obere Grenze ist für die Summen* (2) *bei willkürlicher Annahme der Theile* δ_r, *deren Summe jedoch stets* $\beta - \alpha$ *sein muss.* Dieser auch für uns wünschenswerthe Satz ergiebt sich folgendermaassen. Angenommen jene Grenze sei G. Auch wenn alle Theile δ_r kleiner als die S. 26 angegebene Zahl Δ sind, lässt sich die Summe (2) noch vergrössern. Also ist G auch die obere Grenze für die Summen (2) unter der Voraussetzung, dass ein jedes δ_r kleiner ist als Δ. Nun ist nach (b) S. 26 unter dieser Bedingung

$$-\epsilon < L - \sum_{r=1}^{n} |A_{r-1} A_r| \lesssim \epsilon. \tag{3}$$

Da aber

$$\sum_{r=1}^{n} |A_{r-1} A_r| < G$$

sein soll, so muss $L - \epsilon < G$ oder $L - G < \epsilon$ sein. Hieraus ergiebt sich bei der Willkürlichkeit der positiven Zahl ϵ, dass

$$L \leqq G \tag{4}$$

* Presented to the Society (Chicago) March 29, 1902. Received for publication February 25, 1902.

† Vgl. *Cours d'Analyse*, 2. éd., t. I, Nr. 105–111 (in der Hauptsache schon bei L. SCHEEFFER, Acta Mathematica, t. 5. S. 54).

ist. Unter den in (3) vorkommenden Summen giebt es mindestens eine

$$\sum_{r=1}^{n'} |A'_{r-1}A'_r| > G - \epsilon.$$

Demnach ist

$$L + \epsilon > G - \epsilon, \quad \text{d. i.,} \quad 2\epsilon > G - L,$$

so dass $G \leqq L$ sein muss. Aus dieser und der Beziehung (4) folgt die Gleichung $G = L$.

Wir finden weiter bei JORDAN die *nothwendige und hinreichende* Bedingung dazu, dass für den Bogen (1) ein endlicher Grenzwerth L vorhanden ist. Sie lautet: 1) $\phi(t)$ und $\psi(t)$ müssen Functionen mit endlicher Totaländerung (à variation bornée) im Intervalle (α, β) sein; 2) der Punkt $\big(\phi(t), \psi(t)\big)$ muss auf der geraden Strecke liegen, welche die Punkte

$$\big(\phi(t-0), \psi(t-0)\big), \quad \big(\phi(t+0), \psi(t+0)\big)$$

verbindet.

Hierauf stellt er den Satz auf: „Dazu dass der Bogen s zwischen den den Werthen a und t entsprechenden Punkten der Curve (1) eine stetige Function von t ist, ist nothwendig und hinreichend, dass die Functionen $\phi(t)$ und $\psi(t)$ bei diesem Werthe t stetig seien.“

Dann folgt bei JORDAN der Satz: „Haben die Functionen $\phi(t)$, $\psi(t)$ bei einem Werthe t stetige Differentialquotienten $\phi'(t)$, $\psi'(t)$, so ist

$$\frac{ds}{dt} = \sqrt{\phi'(t)^2 + \psi'(t)^2}.\text{“} \tag{5}$$

Dabei ist natürlich vorausgesetzt, dass der Bogen der Curve (1), welches dem den Werth t enthaltenden Intervalle (α, β) entspricht, eine Länge besitze.

Unter welchen Umständen hat nun dieser Bogen im Falle, dass *beide Functionen $\phi(t)$, $\psi(t)$ im Intervalle (α, β) von t durchweg stetig sind*, eine Länge? Nach dem soeben Bemerkten dann und nur dann, wenn der Gesammtbetrag der Änderung jeder von ihnen im Intervalle (α, β) endlich ist. Dies findet statt,* wenn

(1) die beiden Functionen im Intervalle (α, β) *abtheilungsweise monoton*† d. h. in jedem von gewissen, in endlicher Anzahl vorhandenen Theilen, welche zusammen das Intervall (α, β) ausmachen, monoton sind;

(2) $\phi'(t)$ und $\psi'(t)$ entweder im Intervalle (α, β) von t durchweg stetig sind oder dieses so in eine endliche Anzahl von Theile zerlegt werden kann, dass in jedem von ihnen sowohl $\phi'(t)$, als auch $\psi'(t)$ durchweg stetig ist (vgl. Nr. 7).

---

* Darauf geht JORDAN, a. a. O. nicht ein.

† Nach C. NEUMANN, *Über die nach Kreis- Kugel- und Cylinderfunctionen fortschreitenden Entwickelungen* (1881), S. 26.

Fassen wir zunächst den zweiten Fall in's Auge, so können wir nunmehr aus der Formel (5) unmittelbar die Sätze in Nr. 6 und Nr. 10 ableiten.

Nehmen wir jetzt an, dass die Differentialquotienten $\phi'(t)$, $\psi'(t)$ in jedem Intervalle (a, t'), wo $a < t' < \beta$ ist, durchweg stetig, jedoch mindestens einer von ihnen im ganzen Intervalle (a, β) nicht endlich sei. Haben dann die Gleichungen

$$\phi'(t) = 0, \quad \psi'(t) = 0$$

im Intervalle (a, β) nur eine bestimmte Anzahl von Wurzeln, so sind die Functionen $\phi(t)$, $\psi(t)$ darin abtheilungsweise monoton. Bedeuten A, B, T' die den Werthen $t = a, \beta, t'$ entsprechenden Punkte der Curve (1), so haben die Bogen AT' und AB mithin eine Länge. Und zwar ist nach dem Vorstehenden

$$(6) \qquad s' = \text{arc } AT' = \int_a^{t'} \sqrt{\phi'(t)^2 + \psi'(t)^2}\, dt.$$

Da nun arc $AB = \underset{t'=\beta}{\mathrm{L}}$ arc AT' ist, so finden wir aus (6)

$$(7) \qquad \text{arc } AB = \underset{t'=\beta}{\mathrm{L}} \int_a^{t'} \sqrt{\phi'(t)^2 + \psi'(t)^2}\, dt = \int_a^{\beta} \sqrt{\phi'(t)^2 + \psi'(t)^2}\, dt,$$

dass also das letzte, *uneigentliche Integral vorhanden ist.* Wenn dasselbe durch eine passende Substitution für t sich in ein eigentliches Integral überführen lässt, so ergiebt sich die Formel (7) auch aus dem Satze in Nr. 6.

Eine ähnliche Bemerkung kann man im Falle machen, dass das Intervall (a, β) in eine endliche Anzahl von Theilen zerfällt, in deren jedem $\phi'(t)$, $\psi'(t)$ sich so verhalten, wie gerade angegeben wurde.

Für den Inhalt einer windschiefen Fläche hat JORDAN, wie er in der Vorrede zum I. B. seines Cours selbst sagt, keine befriedigende Erklärung aufgestellt.

PROOF OF THE SUFFICIENCY OF JACOBI'S CONDITION FOR A PERMANENT SIGN OF THE SECOND VARIATION IN THE SO-CALLED ISOPERIMETRIC PROBLEMS*

BY

OSKAR BOLZA

§ 1. *Formulation of the Problem.*

The discussion of the second variation for the simplest class of isoperimetric problems†, in parameter representation, leads to the following question:

Let H_1, H_2, T be three given functions‡ of t, regular in an interval§ (t_0, t_1); moreover it is supposed that $H_1 > 0$ and $T \not\equiv 0$ on (t_0, t_1). *Under what conditions will the definite integral*

$$\delta^2 I = \int_{t_0}^{t_1} \left[H_1 \left(\frac{dw}{dt} \right)^2 + H_2 w^2 \right] dt$$

---

* Presented to the Society (Chicago) March 29, 1902. Received for publication April 2, 1902. Published simultaneously in the *Decennial Publications of the University of Chicago.*

† The class treated in KNESER'S *Lehrbuch der Variationsrechnung* in Chap. IV, in which it is required to minimize an integral of the form

$$I = \int_{t_0}^{t_1} F(x, y, x', y')\, dt\,,$$

while at the same time another integral of the same form

$$K = \int_{t_0}^{t_1} G(x, y, x', y')\, dt$$

has a prescribed value.

‡ H_1, H_2 are derived from $H = F + \lambda G$ in the same manner as F_1, F_2 from F in the theory of the unconditioned problem; for WEIERSTRASS' explicit expression of F_2 see BLISS, Transactions of the American Mathematical Society, vol. 3 (1902), p. 133. Further

$$T = G_{xy'} - G_{x'y} + G_1 (x'y'' - x''y')\,,$$

the literal subscripts denoting partial differentiation.

§ The notation implies that $t_0 < t_1$.

be positive for all functions w, not identically zero, satisfying the following conditions:

(*a*) $$w(t_0) = 0, \qquad w(t_1) = 0,$$

(*b*) $$\int_{t_0}^{t_1} wT\,dt = 0,$$

(*c*) *the functions w satisfy certain conditions concerning continuity and existence and continuity of the first derivative.*

With respect to (*c*) we make the assumption * that w itself shall be continuous on (t_0, t_1) and that the interval (t_0, t_1) can be divided into a finite number of subintervals such that on each subinterval the first derivative exists and is continuous,—with the understanding that in the lower (upper) endpoint of each subinterval "progressive (regressive) derivative" is substituted for "derivative."

The answer is as follows: Denote by $\Psi(w)$ the differential expression

$$\Psi(w) = H_2 w - \frac{d}{dt}\left(H_1 \frac{dw}{dt}\right),$$

and by U and V two integrals † of the differential equations

(1) $$\Psi(U) = 0, \qquad \Psi(V) = T$$

respectively, which vanish for $t = t_0$:

(2) $$U(t_0) = 0, \qquad V(t_0) = 0;$$

further let

$$M = \int_{t_0}^{t} UT\,dt, \qquad N = \int_{t_0}^{t} VT\,dt,$$

and put

$$\Delta(t, t_0) = MV - NU.$$

Then if t_0' denote the zero of $\Delta(t, t_0)$ next greater than t_0 (the "*conjugate to* t_0"), *the necessary and sufficient condition for the validity of the relation* $\delta^2 I > 0$ *is that*

(3) $$t_1 < t_0'.$$

---

* This agreement means for the isoperimetric problem that we restrict ourselves to continuous curves made up of a finite number of arcs along each of which the curve has a continuously turning tangent.

† It is well known that the general integral of

$$\Psi(w) = \mu T,$$

where μ is any constant, can be derived from the general integral of the differential equation of the extremals by differentiation with respect to the constants of integration and the isoperimetric constant λ. See HORMANN, Dissertation, Göttingen, 1887, and KNESER, Mathematische Annalen, vol. 55 (1901), p. 93.

That this condition ("Jacobi's condition") is *necessary* is easily seen.* For the integral $\delta^2 I$ can be thrown, by an integration by parts, into the form

$$\delta^2 I = \int_{t_0}^{t_1} w \Psi(w)\, dt, \tag{4}$$

so that, on account of (b),

$$\delta^2 I = \int_{t_0}^{t_1} w \left(\Psi(w) - \mu T\right) dt, \tag{5}$$

μ being any constant. And if $t_0' \gtrless t_1$, we could make $\delta^2 I = 0$ by choosing

$$\begin{aligned} &\mu = M(t_0'), \\ &w = M(t_0')V(t) - N(t_0')U(t) \quad \text{on} \quad (t_0, t_0'), \\ &w \equiv 0 \qquad\qquad\qquad\qquad\quad \text{on} \quad (t_0', t_1); \end{aligned}$$

this function w fulfills the conditions (a), (b), (c) and besides it satisfies the differential equation

$$\Psi(w) = M(t_0')T,$$

and therefore it makes $\delta^2 I = 0$.†

It is less evident that the condition (3) is also *sufficient*, and to show this is the object of the present note.

§ 2. *Proof‡ of the Sufficiency of Jacobi's Condition.*

Our proof is based upon an extension of the lemma concerning the differential expression $\Psi(w)$ by which JACOBI proves the analogous theorem for the unconditioned problem, viz:

---

*Compare HORMANN, l. c., and KNESER, l. c.; the proof had already been given, in slightly different form, in WEIERSTRASS' Lectures on the Calculus of Variations of 1872.

† $\delta^2 I$ can even be made < 0, as shown by KNESER, l. c.; compare also BOLZA, *Zur zweiten Variation bei isoperimetrischen Problemen*, in one of the forthcoming numbers of the Mathematische Annalen.

‡ Inasmuch as the isoperimetric problem here considered is a special case of the general problem: To minimize an integral of the form

$$I = \int_{t_0}^{t_1} F(t;\, x_1, x_2, \cdots, x_n;\, x_1', x_2', \cdots, x_n')\, dt,$$

the unknown functions $x_1, x_2, \cdots, x_n$ being connected by a number of relations of the form:

$$\phi_\alpha(t;\, x_1, x_2, \cdots, x_n;\, x_1', x_2', \cdots, x_n') = 0 \qquad (\alpha = 1, 2, \cdots, m),$$

the proof might be derived by specialization from MAYER's researches on the second variation for the general problem (Crelle's Journal, vol. 69 (1868), p. 238, and Mathematische Annalen, vol. 13 (1878), p. 53; compare also C. JORDAN, *Cours d'Analyse*, III, Nos. 373–394 and v. ESCHERICH, Sitzungsberichte der Wiener Academie, vol. 107, II_a (1898), pp. 1191, 1268, 1384). A proof thus obtained would, however, be much more complicated than the direct proof given in the text.

If u be any integral of the differential equation

$$\Psi(u) = 0,$$

then for every function p admitting first and second derivatives the relation

$$(pu)\Psi(pu) = H_1(p'u)^2 - \frac{d}{dt} H_1 pp'u^2$$

holds, accents denoting differentiation with respect to t.

To obtain the desired extension of this lemma let u, v be integrals of the differential equations

$$\Psi(u) = 0, \qquad \Psi(v) = T \tag{6}$$

respectively, both vanishing in a point $t = \tau_0$:

$$u(\tau_0) = 0, \qquad v(\tau_0) = 0; \tag{7}$$

let further p, q be two arbitrary functions of t admitting first and second derivatives, and denote for shortness

$$\omega = pu + qv.$$

Then

$$\omega\Psi(\omega) = (pu + qv)qT - H_1(pu + qv)(p'u' + q'v') - (pu + qv)\frac{d}{dt} H_1(p'u + q'v),$$

which may easily be written

$$\omega\Psi(\omega) = H_1(p'u + q'v)^2 - H_1(pq' - p'q)(uv' - u'v) + (pu + qv)qT - \frac{d}{dt} H_1(pu + qv)(p'u + q'v).$$

Further if we introduce

$$m = \int_{\tau_0}^{t} uT\,dt, \qquad n = \int_{\tau_0}^{t} vT\,dt,$$

then

$$(pu + qv)qT = (pm' + qn')q = \frac{d}{dt}(pm + qn)q - (p'm + q'n)q - (pm + qn)q'.$$

But from (6) and (7) follows that *

$$H_1(uv' - u'v) = -m;$$

hence we obtain

$$(pu+qv)\Psi(pu+qv) = H_1(p'u+q'v)^2 - 2q(p'm+q'n) - \frac{d}{dt}[H_1(pu+qv)(p'u+q'v) - (pm+qn)q], \tag{8}$$

which is the desired extension of JACOBI's lemma.

Since

$$H_1\omega'^2 + H_2\omega^2 = \omega\Psi(\omega) + \frac{d}{dt}(H_1\omega\omega'),$$

we further derive from (8) the following relation:

$$H_1\omega'^2 + H_2\omega^2 = H_1(p'u+q'v)^2 - 2q(p'm+q'n) + \frac{d}{dt}[H_1(pu+qv)(pu'+qv') + (pm+qn)q]. \tag{9}$$

In the latter formula the second derivatives of p and q do not occur; hence it can be inferred that (9) *holds even for functions* p, q *admitting first but not second derivatives.*—

We now proceed to prove the sufficiency † of JACOBI's condition. We suppose then that

$$t_1 < t_0',$$

so that

$$\Delta(t, t_0) \neq 0 \qquad \text{for every } t, \qquad t_0 < t \leqq t_1.$$

Now choose $\tau_0 < t_0$ but so near to it that H_1, H_2, T remain regular in the enlarged interval (τ_0, t_1) and that

$$\Delta(t, \tau_0) \neq 0, \tag{10}$$

for every t, $t_0 \leqq t \leqq t_1$; such a choice of τ_0 is always possible. ‡

---

* Compare KRESER, l. c., equation (22).

† It is hardly necessary to say that we are always speaking of sufficiency *for a permanent sign of* $\delta^2 I$, not of sufficiency *for a minimum*.

‡ For a proof see C. JORDAN, *Cours d'Analyse*, vol. III, no. 393.

Let w be any function of t satisfying the conditions (a), (b), (c) for the interval (t_0, t_1) and $\equiv 0$ on (τ_0, t_0); then define the two functions p, q by the two equations

$$\begin{aligned} pu + qv &= w, \\ p'm + q'n &= 0, \end{aligned} \tag{11}$$

with the initial condition

$$p(t_0) = 0, \qquad q(t_0) = 0. \tag{12}$$

But from (11) it follows that

$$\frac{d}{dt}(pm + qn) = (pu + qv)\,T = wT,$$

hence integrating and remembering (12), we obtain

$$pm + qn = \int_{t_0}^{t} wT\,dt. \tag{13}$$

We thus obtain for the determination of p, q two linear equations whose determinant is

$$mv - nu = \Delta(t, \tau_0),$$

and therefore $\neq 0$ on (t_0, t_1) according to (10); hence p and q are continuous on (t_0, t_1) and with respect to their derivatives of the same character as w.

For the same reason p and q, both vanish not only in t_0, but also in t_1, since according to (a) and (b), w and

$$\int_{t_0}^{t} wT\,dt$$

vanish in t_0 *and in* t_1. Using these functions p and q in the transformation (9) and integrating * between the limits t_0 and t_1 we obtain the *final result:*

$$\delta^2 I = \int_{t_0}^{t_1} H_1(p'u + q'v)^2\,dt. \tag{14}$$

This proves that indeed

$$\delta^2 I > 0$$

* If w', and accordingly p' and q', have discontinuities of the kind admitted by our assumptions, the integral would have to be broken up into a sum of integrals taken over the subintervals; but as p and q themselves are continuous, formula (9) shows that (14) remains true also in this case.

for all functions w satisfying the conditions (a), (b), (c), *provided* $t_1 < t_0'$. For $\delta^2 I > 0$ unless $p'u + q'v$ were identically zero; but then it would follow from $p'm + q'n = 0$ and (10) that p' and q' must vanish identically and therefore also p and q themselves since they vanish in t_0 and are continuous; but this is against the assumption that w does not vanish identically.

THE UNIVERSITY OF CHICAGO, *April* 2, 1902.

ON HYPERCOMPLEX NUMBER SYSTEMS*

BY

HERBERT EDWIN HAWKES

Introduction.

The theories of hypercomplex numbers and of continuous groups were first explicitly connected by POINCARÉ† in 1884 with the statement that the problem of complex numbers was reduced to that of finding all the linear continuous group of substitutions in n variables of which the coefficients are linear functions of n arbitrary parameters, and since that time the advance in the theory of hypercomplex numbers has been largely suggested by the theory of continuous groups. In 1889 STUDY‡ and SCHEFFERS§ developed the relation between these theories to a considerable extent, and the latter‖ in 1891 arrived at a complete enumeration of systems in less than six units which are inequivalent (of different "Typus"), non-reciprocal, irreducible, and which possess moduli. Previously (1889) STUDY¶ had enumerated all inequivalent systems with moduli in less than five units without direct use of the theory of continuous groups, and in 1890 ROHR** continued the work through systems in five units.

The problem of enumerating hypercomplex number systems had been attacked by BENJAMIN PEIRCE about twenty years before the investigations of STUDY and SCHEFFERS. His results were not printed, however, until after his death.††

With the methods of the European investigators in mind, I have else-

* Presented to the Society at the New York meeting, June 28, 1900. Received for publication October 1, 1900, and, as modified, September 15, 1901.

† Comptes Rendus, vol. 99, p. 740, 1884.

‡ Leipziger Berichte, p. 177, 1889.

§ Leipziger Berichte, p. 400, 1889.

‖ Mathematische Annalen, vol. 39, p. 293, 1891.

¶ Göttinger Nachrichten, p. 237, 1889; Monatshefte für Mathematik und Physik, vol. 1, p. 283, 1890.

** Dissertation, Marburg, *Ueber die aus 5 Haupteinheiten gebildeten komplexen Zahlensysteme*, 1890.—To afford a basis for a rough estimate of the comparative directness of the various methods of enumeration it may be noted that SCHEFFERS' memoir contains 87 pages, while the portion of STUDY's memoir (Monatshefte) concerned in the enumeration and ROHR's dissertation together contain 81 pages.

†† American Journal of Mathematics, vol. 4, p. 97, 1881.—In 1870 PEIRCE published his work in lithographed form. This publication was reviewed by SPOTTISWOODE in 1872 in the Proceedings of the London Mathematical Society, vol. 4, p. 147. However, since this lithographed edition was small, PEIRCE's work was not easily accessible to mathematicians until 1881.

where * closely scrutinized PEIRCE's memoir, which for many years has been subject to neglect or adverse criticism. In this paper I propose to show that by using PEIRCE's principles as a foundation we can deduce a method more powerful than those hitherto given for enumerating all number systems of the types SCHEFFERS has considered. Theorems V, VI, X, XI are, I believe, new. It is in the first two of these theorems that the ease and directness of this method appear. Those of PEIRCE's theorems which I have needed I have not hesitated to prove. This has been done partly to make the paper complete in itself, and partly to place PEIRCE's work on a clear and rigorous basis.

Definitions.†

Let a and β be any two numbers of an hypercomplex number system.

Def. 1. If $a\beta = \beta a = a$, a is an *idemfactor* with respect to β.

Def. 2. If $\beta a = a$, a is *idemfaciend* with respect to β.

Def. 3. If $a\beta = a$, a is *idemfacient* with respect to β.

Def. 4. If $\beta a = a\beta = 0$, a is a *nilfactor* with respect to β.

Def. 5. If $\beta a = 0$, a is *nilfaciend* with respect to β.

Def. 6. If $a\beta = 0$, a is *nilfacient* with respect to β.

Def. 7. If for the number a a positive integer n exists so that $a^n = 0$, a is *nilpotent.*

Def. 8. If the non-zero number a is equal to its square: $a^2 = a$, a is *idempotent.*

I.

IDEMPOTENT SYSTEMS.

THEOREM I.‡ *In every n-tuple number system, in which not every number is a divisor of zero, there exists an idempotent number.*

Let a be any number not a divisor of zero. Then there exists a non-zero number γ such that

$$a\gamma = a. \tag{1}$$

This number γ is an idempotent number, for we have:

$$a\gamma^2 = a\gamma,$$

and so indeed:

$$\gamma^2 = \gamma. \tag{2}$$

Here we have used the theorem§ that any two numbers a, β of which a is not a divisor of zero serve to determine a definite number $x = \xi$ of the number system, which satisfies the equation:

* American Journal of Mathematics, vol. 24, 1902.

† PEIRCE, loc. cit., p. 104.

‡ This theorem is stated by PEIRCE, loc. cit., p. 109.

§ Cf., e. g., BERLOTY'S thesis, *Théorie des Quantités Complexes à n Unités Principales*, p. 19, 1886, Paris.

$$ax = \beta.$$

Def. 9. A number system which contains an idempotent number is an *idempotent system.*

Def. 10. A number system which contains no idempotent number is a *nilpotent system.*

For the present we deal with idempotent systems.

The units of any idempotent system may be transformed by the equations

$$e_k' = \sum_{i=1}^{n} a_{ik} e_i, \quad e_n' = \gamma \qquad (k=1, \cdots, n-1),$$

so that the new unit e_n is idempotent. We assume in every case that this transformation has been made. The coefficients a_{ik} may have any values such that the determinant of the equations of transformation does not vanish.

THEOREM II.* *All the units of an n-tuple system with one idempotent unit e_n may be chosen so as to fall into the following groups:*

GROUP I *contains units e_k which are idemfactors with respect to e_n. Thus $e_k e_n = e_n e_k = e_k$. This group is symbolized by (dd).*

GROUP II *contains units e_k which are idemfaciend and nilfacient with respect to e_n. Thus $e_n e_k = e_k$, $e_k e_n = 0$. This group is symbolized by (dn).*

GROUP III *contains units e_k which are nilfaciend and idemfacient with respect to e_n.* Thus $e_k e_n = e_k$, $e_n e_k = 0$. *This group is symbolized by (nd).*

GROUP IV *contains units e_k which are nilfactors with respect to e_n. Thus $e_k e_n = e_n e_k = 0$. This group is symbolized by (nn).*

The proof falls into two parts.

[A] *The units of an idempotent number system S may be so chosen as to be either idemfaciend or nilfaciend with respect to e_n.*

Any number a of S is in one of two classes:

(a) A number β exists such that $e_n\beta = a$.

(b) No such number β exists.

Consider numbers a in class (a):

$$e_n a = e_n^2 \beta = e_n \beta = a.$$

Thus all numbers of (a) are idemfaciend with respect to e_n. Suppose there are $n - r$ independent numbers of this class. Transform the system so that these numbers are the units $e_{r+1} e_{r+2} \cdots e_n$ of which we still assume that e_n is idempotent. Any number of (a) contains only those units or else we should have numbers in (a) independent of $e_{r+1} e_{r+2} \cdots e_n$. Thus $e_1 \cdots e_r$ may be any properly chosen numbers independent of $e_{r+1} e_{r+2} \cdots e_n$. These units may be taken nilfaciend with respect to e_n. For since they are not of (a),

* PEIRCE, loc. cit., p. 109.

$$e_n e_k = \gamma + \delta \qquad (k \leqq r),$$

where

$$\gamma = \sum_{i=1}^{r} a_i e_i, \quad \delta = \sum_{i=r+1}^{n} a_i e_i.$$

If $\gamma \neq 0$, then $e_n(e_k - \delta) = \delta + \gamma - \delta = \gamma$, and γ is in (a) which is impossible.

We have, therefore, $\gamma = 0$.

Let now

$$e_i' = e_i - \sum_{s=r+1}^{n} \gamma_{nis} e_s \qquad (i = 1, 2, \cdots, r),$$

$$e_i' = e_i \qquad (i = r+1, \cdots, n).$$

where γ_{nis} are some of the constants of multiplication * of the system.

Then

$$e_n' e_i' = e_n e_i - \sum_{s=r+1}^{n} \gamma_{nis} e_s = \sum_{s=r+1}^{n} \gamma_{nis} e_s - \sum_{s=r+1}^{n} \gamma_{nis} e_s = 0 \qquad (i = 1, 2, \cdots r),$$

$$e_n' e_k' = e_n e_k = e_k = e_k' \qquad (k = r+1, \cdots, n).$$

It is clear that the new units $e_1', \cdots e_n'$ are independent.

Thus [A] is established.

[B] *Without disturbing the property of the units just established we can so transform our system that the new units are either nilfacient or idemfacient with respect to* e_n.

We observe that

(3) $$e_\lambda e_n = \sum_{s=1}^{r} \gamma_{\lambda ns} e_s \qquad (\lambda = 1, \cdots, r),$$

(4) $$e_\nu e_n = \sum_{s=r+1}^{n} \gamma_{\nu ns} e_s \qquad (\nu = r+1, \cdots, n).$$

For let

$$e_\lambda e_n = \sum_{s=1}^{n} \gamma_{\lambda ns} e_s \qquad (\lambda = 1, \cdots, r).$$

By the associative law,

$$e_n e_\lambda \cdot e_n = 0 = e_n \cdot e_\lambda e_n = \sum_{s=r+1}^{n} \gamma_{\lambda ns} e_s \qquad (\lambda = 1, \cdots, r).$$

Thus

$$\gamma_{\lambda ns} = 0 \qquad (\lambda = 1, \cdots, r;\ s = r+1, \cdots, n),$$

which establishes (3). By similar use of the associative law on the product $e_n e_\nu e_n (\nu = r+1, \cdots, n)$ we verify (4).

* The n^3 constants γ_{iks} which occur in the equations

$$e_i e_k = \sum_{s=1}^{n} \gamma_{iks} e_s \qquad (i, k = 1, \cdots, n)$$

we call (after HAMILTON) constants of multiplication.

The units of our system are now in two groups, $e_1 \cdots e_r$ and $e_{r+1} \cdots e_n$, and are subject to [A] and equations (3) and (4). We can now use the proof of [A], with interchange of the order of multiplication of e_n and e_k, *inside* the group $e_1 \cdots e_r$ to show that the units of that group may be so transformed as to be idemfacient or nilfacient with respect to e_n. The same process may be applied to the set of units $e_{r+1} \cdots e_n$ with a similar result. Thus the units of our system fall into the four required groups. Evidently e_n is in group I.

THEOREM III.* *The group of the non-vanishing product of any two units of the various groups is shown by the following table:*

	nn	*nd*	*dn*	*dd*
nn	*nn*	*nd*	0	0
nd	0	0	*nn*	*nd*
dn	*dn*	*dd*	0	0
dd	0	0	*dn*	*dd*

The multiplier is in the left hand column of the above table.

For example: take e_k from group III or (nd), and e_j from group II or (dn). Then

$$e_n e_k e_j = 0 = e_k e_j e_n,$$

since e_k is nilfaciend, and e_j is nilfacient. Thus the product is in group IV or (nn), provided it does not vanish. Similarly each product of the table may be verified.

Def. 11. When the units of a system satisfy the conditions indicated by the table we call the system *regular* with respect to the unit e_n.

From an inspection of the regular table it appears that idempotent units can exist only in groups I or IV. If e_n is the modulus, † the system can contain only units of group I.

THEOREM IV.‡ *If there are two or more independent idempotent numbers in group* I, *the system may be transformed without disturbing its regularity so that e_n is the only idempotent number in group* I.

Let S denote the system $e_1, \cdots, e_n$, regular with respect to e_n, of which $e_1, \cdots, e_r, e_n$ are in group I thus constituting a system S_1 by themselves. Let a be a number in S_1 independent of e_n such that $a^2 = a$. Transform S by the equations

$$e_i' = \sum a_{ij} e_j, \qquad (i = 1, 2, \cdots, n-1);$$

$$e_n' = e_n - a,$$

* PEIRCE, loc. cit., p. 111.

† See def. 13.

‡ PEIRCE, loc. cit., p. 112.

where the a's are so chosen that the determinant of the system does not vanish. By theorem II we may so choose $e'_1, e'_2, \cdots, e'_{n-1}$ that each falls into one of the four groups I, II, III, IV, with respect to e'_n.

But from the table it appears that no expression linear in the old units can be idemfactorial with respect to e'_n except an expression linear in $e_1, e_2, \cdots, e_r, e_n$, alone. Thus the units of S in group I with respect to e'_n are the same, or may be so chosen, as the units of S_1 in group I with respect to e'_n. At least one of the units of S_1 is in group IV with respect to e'_n, since there is a number linear in $e_1, \cdots, e_r, e_n$, namely, a nilfactorial with respect to e'_n. Therefore the first group of S_1 and hence the first group of S with respect to e'_n contains at most only r units, whereas group I with respect to e_n contained $r+1$ units. In this way whenever group I contains two independent idempotent numbers we may transform the system so as to reduce by at least one the number of units in that group.

THEOREM V. *If there is an idempotent number in group* IV *it may be taken as a unit, and the whole system made regular with respect to it without disturbing the regularity with respect to* e_n.

Let e_{n-1} be the idempotent unit of group IV. Let e_k $(k = r+1, \cdots, s)$ be units of group II. Then one has

$$e_{n-1}e_k = 0, \qquad e_k e_{n-1} = \sum_{i=r+1}^{s} \gamma_{k\,n-1\,i} e_i,$$

by the table of theorem III. We must now transform our system so that the new units e'_k, are in group II with respect to e_n but in group III or IV with respect to e_{n-1}, that is, so that $e'_k e_{n-1} = 0$ or e'_k. But since the units in the original group II together with e_{n-1} form a system by themselves, we can, in fact, use the method of proof [A] to show that the units of group II with respect to e_n can be so transformed that the new units are either idemfacient or nilfacient with respect to e_{n-1}, and consequently fall in group III or IV with respect to that unit. Since the transformations involve only units in the original group II the regularity with respect to e_n is not affected. We can proceed similarly to show that group III with respect to e_n may be so transformed as to contain only units of group II or IV with respect to e_{n-1}. Group I with respect to e_n is evidently in group IV with respect to e_{n-1}. Theorem II may be repeated to show that the units in group IV with respect to e_n may be so chosen as to fall into the four groups with respect to e_{n-1}. This again does not affect the regularity of the system since the equations of transformation involve only units of IV. We denote the four groups with respect to e_{n-1} by I_1, II_1, III_1, IV_1. We also see that all units of I_1 are in IV, all units of II_1 are in III or IV, units of III_1 are in II or IV, and units of IV_1 are in I, II, III, or IV.

Let the idempotent units be represented by $e_{n-t+1}, \cdots, e_n$.

THEOREM VI. *The system remaining regular with respect to* e_n *and* e_{n-1} *can be so transformed that only one idempotent unit remains in* I_1 *and* I *respectively. All the other idempotent numbers pass to* IV_1. *The system retaining its regularity can then be transformed so as to be regular with respect to any one of these idempotent units of* IV_1 *as* e_{n-2}.

The first part of this theorem is proved by the method used in theorem IV. The second part is shown by an essential repetition of theorem V.

This process may be continued as long as two independent units remain in any group IV. We finally have our system regular with respect to each of the idempotent units. Let the four groups into which the units fall with respect to e_{n-k} be denoted by I_k, II_k, III_k, IV_k. Each group I_k contains one and only one idempotent number, namely e_{n-k}. The product of any two distinct idempotent units vanishes since any such unit is in group IV with respect to every other idempotent unit. We are now able to form a general table of the relations of the various groups to one another. Since I_2 consists of units which are idemfactors with respect to a unit which is in IV_1 and IV, all units in I_2 must be in IV_1 and IV. Units in II_2 may be in III_1 or IV_1. Units in III_1 may be in II or IV, but only those units in III_1 which are also in IV can be in II_2 by the table in theorem III. Further only the units in IV_1 which are also in III or IV can be in II_2. Similarly units in III_2, which may contain units in II_1 and IV_1, can contain only units common to II_1 and IV, and units common to IV_1 and II or IV. In this way we arrive at the following tables. Units in a certain group with respect to e_{n-k} are also in the group found on the same line reading toward the right.

I_k	IV_{k-1}	IV_{k-2}	$\cdots$	IV
II_k	$III_{k-1}\ IV_{k-1}$	$III_{k-2}\ IV_{k-2}$	$\cdots$	III IV
III_k	$II_{k-1}\ IV_{k-1}$	$II_{k-2}\ IV_{k-2}$	$\cdots$	II IV
IV_k	$I_{k-1}\ II_{k-1}\ III_{k-1}\ IV_{k-1}$	$I_{k-2}\ II_{k-2}\ III_{k-2}\ IV_{k-2}$	$\cdots$	I II III IV

I_k	IV_{k+1}	IV_{k+2}	$\cdots$	IV_{n-t+1}
II_k	$III_{k+1}\ IV_{k+1}$	$III_{k+2}\ IV_{k+2}$	$\cdots$	$III_{n-t+1}\ IV_{n-t+1}$
III_k	$II_{k+1}\ IV_{k+1}$	$II_{k+2}\ IV_{k+2}$	$\cdots$	$II_{n-t+1}\ IV_{n-t+1}$
IV_k	$I_{k+1}\ II_{k+1}\ III_{k+1}\ IV_{k+1}$	$I_{k+2}\ II_{k+2}\ III_{k+2}\ IV_{k+2}$	$\cdots$	$I_{n-t+1}\ II_{n-t+1}\ III_{n-t+1}\ IV_{n-t+1}$

LIMITATION TO SYSTEMS WITH MODULI.—From the two preceding tables we see that *in a system thus regularized, which moreover contains for no index* k $(k = 0, \cdots, t-1)$ *units in a group* II_k, III_k, *or* IV_k *and at the same time in every group* IV_σ $(\sigma = 0, \cdots, t-1;\ \sigma \neq k)$, *there exists for every* $e_\rho (\rho = 1, \cdots, n-t)$ *one and only one pair of integers* $(\lambda\lambda_1)$, *where* $t-1 \geqq \lambda$, $\lambda_1 \geqq 0$, *such that*

$$e_\rho e_{n-\lambda_1} = e_\rho; \quad e_{n-\lambda} e_\rho = e_\rho.$$

If e_ρ is in I_k, evidently $\lambda_1 = \lambda = k$.

Def. 12. We call the pair of integers $(\lambda\lambda_1)$ which corresponds in this way to e_ρ the *character* * of e_ρ.

We consider henceforth only idempotent systems satisfying the condition italicized above, and proceed to show that these are exactly the systems with moduli.

Def. 13. A number μ of a system S is *a modulus* if for every a of the system

$$a\mu = \mu a = a. \tag{5}$$

Note. If μ and μ' are moduli of a system S, then by definition (5)

$$\mu\mu' = \mu, \quad \mu\mu' = \mu', \tag{6}$$

and so $\mu = \mu'$. Thus one speaks of *the modulus* of a system.

Now one sees immediately that in the systems under consideration the number

$$\mu = \sum_{k=1}^{t} e_{n-t+k}$$

is a modulus. (One speaks of a system with a modulus in t idempotent units.)

Further no system so far excluded has a modulus. For a system with a modulus is an idempotent system, and no idempotent system excluded by the condition in question has a modulus. For in such a system let, for example, e_λ be a unit which is simultaneously in the groups $\mathrm{III}_k\,(0 \leqq k \leqq t-1)$ and in the groups $\mathrm{IV}_\sigma\,(\sigma = 0, \cdots, t-1; \sigma \neq k)$. A modulus if existent is idempotent and a linear combination of $e_{n-t+1}, \cdots, e_n$. For the modulus if existent must contain all these idempotent units, and can contain no other number. But since e_λ is nilfaciend with respect to each of these units, it is nilfaciend with respect to every idempotent number linear in $e_{n-t+1}, \cdots, e_n$. Hence no modulus exists.

LEMMA. *If in any group* I *the idempotent unit does not occur in any product of non-idempotent units, every number in the group not involving the idempotent unit is nilpotent.*

For convenience of notation let the group I comprise the entire system, and let the idempotent unit be e_n. (This is permissible since the product of two units of a group I involves only units of that group.)

Let a be any number in group I not involving e_n. Then some least integer $m \leqq n$ must exist such that

* SCHEFFERS, *Zurückführung complexer Zahlensysteme auf typische Formen*, Mathematische Annalen, vol. 39, p. 313.

$$\sum_{k=1}^{m} a_k a^k = 0 \qquad (a_m \neq 0). \tag{7}$$

If $m = 1$, then a vanishes and is nilpotent. If $m > 1$, two cases arise.

1°) $\qquad a_1 \neq 0.$

Setting

$$\beta = \sum_{k=2}^{m} a_k a^{k-1},$$

we write (7) in the form:

$$0 = a_1 a + \beta a = (a_1 e_a + \beta) a,$$

from which we easily obtain

$$(a_1 e_a + \beta)\beta = 0,$$

or

$$\left(-\frac{\beta}{a_1}\right)^2 = -\frac{\beta}{a_1}.$$

But β does not contain e_a and hence is independent of e_a. Thus, since $\beta \neq 0$, we have in $-\beta/a_1$ a second idempotent number in the group. But this is impossible. Thus the case 1°) does not occur.

2°) $\qquad a_k = 0, \quad a_\lambda \neq 0 \qquad (k = 1, \cdots, \lambda - 1;\ \lambda \geqq 2).$

Then

$$\sum_{i=\lambda}^{m} a_i a^i = 0. \tag{8}$$

We set $m = \lambda + \nu$.

If $\nu = 0$, then $a^m = 0$ and a is nilpotent.

If $\nu > 0$, there is an equation of degree m':

$$\sum_{k=1}^{m'} b_k \beta^k = 0 \qquad \begin{pmatrix} 1 + \nu \geqq m' \geqq \mu \\ b_{m'} \neq 0;\ \beta = a^\lambda \end{pmatrix}; \tag{9}$$

here μ denotes the least integer such that $\mu > 1$, $\lambda\mu \geqq \lambda + \nu$. When this statement is proved, it is apparent that a is nilpotent, for β is a power of a and the equation (9) is of the type of equation (7) but of lower degree, and so in the sequential application of the reasoning leading from (7) to (9) the equations analogous to (9) occur only a finite number of times and when no such equation occurs a certain power of a is recognized as a nilpotent number.

From (8) we have the equations

$$\sum_{i=\lambda}^{\lambda+\nu} a_i a^{i+j} = 0 \qquad (j = 0, 1, 2, \cdots). \tag{8_j}$$

We think of an equation (8_j) as written with powers of $\beta (\beta = a^\lambda)$ thrown to the right and with the other powers of a retained on the left and written in

order of decreasing exponents. The lowest power of a in (8_j) is $a^{\lambda+j}$ and the highest power is $a^{\lambda+\nu+j}$. The first equation (8_j) involving $\beta^\kappa = a^{\lambda\kappa}(\kappa \geqq \mu)$ is the equation $(8_{\lambda\kappa-\lambda-\nu})$.

The system $\{8\}_\kappa$ of $\lambda\kappa - \lambda - \nu + 1 = \rho_\kappa$ equations (8_j), $j = 0, 1, \cdots, \rho_\kappa - 1$, arranged according to ascending values of j, is taken for consideration. This system of equations involves on the right $\beta^1, \cdots, \beta^\kappa$ and on the left homogeneously certain $\rho_\kappa + \nu - \kappa$ powers of a not powers of β.

For this system $\{8\}_\kappa$ we have an eliminant

$$(9_\kappa) \qquad \sum_{k=1}^{\kappa} b_{k\kappa}\beta^k = 0$$

in case every determinant D_κ of order ρ_κ of the array A_κ of the system $\{8\}_\kappa$ vanishes, and indeed one of the type (9), i. e., with $b_{\kappa\kappa} \neq 0$, in case $\rho_\kappa = 1$ or in case of the array A'_κ obtained by omitting the last line of A_κ not every determinant D'_κ of order $\rho_\kappa - 1$ vanishes. The latter condition if fulfilled implies that $\kappa \leqq 1 + \nu$. If $\kappa = 1 + \nu$ the former condition is surely satisfied.

We shall prove that both conditions are satisfied for some value of κ,

$$\kappa = m', \quad \mu \leqq m' \leqq 1 + \nu.$$

The corresponding eliminant (9_κ) is the desired equation (9).

Unless both conditions are satisfied for $\kappa = 1 + \nu$, every (the single) determinant $D'_{1+\nu}$ vanishes. Remembering that $a_{\lambda+\nu} \neq 0$ we see then that every (the single) determinant D_ν vanishes. And if every D'_ν vanishes, then every $D_{\nu-1}$ vanishes. Thus proceeding we see that for some $\kappa = m'(\mu < m' \leqq 1 + \nu)$ every $D_{m'}$ vanishes and not every $D'_{m'}$ vanishes, or else every D_μ vanishes and either $\rho_\mu = 1$ or not every D'_μ vanishes; for if $\rho_\mu > 1$ one determinant D'_μ has the non-zero value $(-1)^{\frac{1}{2}\rho_\mu(\rho_\mu-1)} a_{\lambda+\nu}^{\rho_\mu - 1}$.

Def. 14. The exponent in the highest non-vanishing power of a nilpotent number is called its *degree*.

Def. 15.* If a unit e_k is erased from every position it occupies in a multiplication table, the system is said to be *deleted* by that unit.

THEOREM VII.† *Every number in a nilpotent system is nilpotent.*

Let S be any nilpotent system in $n - 1$ units. Border this system on the right and below by a unit e_n such that $e_k e_n = e_n e_k = e_k$ $(k = 1, \cdots, n)$. We have then a system with no idempotent number independent of e_n, and so of the nature considered in the preceding lemma. Thus the multiplicative properties of the nilpotent system must conform to the condition there established and all its numbers must be nilpotent.

---

* SCHEFFERS, loc. cit., p. 307

† PEIRCE, loc. cit., p. 113.

THEOREM VIII.* *The non-vanishing powers of a nilpotent number are independent.*

Let a be a nilpotent number of degree m. Hence $a^m \neq 0$, $a^t = 0\ (t > m)$. Then if a, a^2, $\cdots$, a^m are not independent they satisfy a linear relation of the form,

$$\sum_{k=r}^{m} a_k a^k = 0 \qquad (a_r \neq 0,\ r \geqq 1). \tag{10}$$

Multiply (10) by a^{m-r} and we get $a_r a^m = 0$; hence $a_r = 0$. Thus no such linear relation exists and the powers of a are seen to be independent. It is often convenient to take for units these independent powers of the unit of highest degree in a system.

THEOREM IX. *The multiplication table of any number system which has a modulus in one idempotent unit, can be transformed so that e_n occurs only in the product e_n^2.*

To any number system with a modulus corresponds a pair of reciprocal, simply transitive projective groups. A system is called non-quaternion or quaternion according as the corresponding groups are integrable or not. The simplest quaternion system is HAMILTON'S system of quaternions, which occurs as a subsystem in every quaternion system.† Since HAMILTON'S system contains two idempotent numbers no quaternion system is considered under the present theorem.

The groups which correspond to non-quaternion systems have the following well known property. Consider the parameters in the equations defining the group to be coördinates of points in space of n dimensions. Then in this space there is one point, one line through the point, one plane through the line, etc., which remain invariant under the group. Considering now a point in space as affording a complex number of our system we can state the corresponding theorem for complex numbers, as follows. There is in our system one number (which we will take for the unit e_1) which, when multiplied by any number in the system remains unchanged except for a constant of multiplication. Thus

$$e_k e_1 = \gamma_{k11} e_1 \qquad (k = 1, 2, \cdots, n).$$

There is also a number e_2 such that the product of any number on it (in the same order as in the previous product) is a linear combination of e_1 and e_2. Thus

$$e_k e_2 = \gamma_{k21} e_1 + \gamma_{k22} e_2, \qquad (k = 2, 3, \cdots, n).$$

Similarly

$$e_k e_l = \gamma_{kl1} e_1 + \gamma_{kl2} e_2 + \cdots + \gamma_{kll} e_l \quad (k, l = 1, 2, \cdots, n;\ k \geqq l)$$

* PEIRCE, loc. cit., p. 114.

† Encyclopädie der Mathematischen Wissenschaften, vol. I, page 181. See also CARTAN, Comptes Rendus, 1897, page 1220.

But to any given system corresponds also a second group reciprocal to the one just considered and from the same reasoning we see that

$$e_l e_k = \gamma_{lk1} e_1 + \gamma_{lk2} e_2 + \cdots + \gamma_{lkl} e_l \quad (k, l = 1, 2, \cdots, n\,;\, k \geqq l).$$

Thus

$$e_i e_k = \sum_{s=1}^{l} \gamma_{iks} e_s$$

where l is the less of i and k.* The single idempotent number of our system is the modulus μ, and must contain e_n. If we now transform our system by the equations

$$e'_k = e_k, \qquad e'_n = \mu \qquad (k = 1, 2, \cdots, n-1),$$

the new units are independent of each other and the theorem is established.

THEOREM X. *Two systems containing different numbers of independent idempotent numbers are inequivalent.*

Let S and S_1 be two systems containing r and $r + s$ independent idempotent numbers respectively which we assume are taken as the units of highest indices. If they were equivalent, we should have

$$e'_{n-k} = \sum_{\lambda=1}^{n} a_{n-k,\lambda} e_\lambda \qquad (k = 0, \cdots, r+s-1),$$

where e'_{n-k} are units in S_1. But since these numbers are idempotent and independent the right-hand members must be the same, which would give us $r + s$ independent idempotent numbers in S; and this is impossible.

Similarly we can show that systems which have been regularized (according o theorem VI) and in which the units fall into groups in different arrangements are inequivalent.

We are now in a position to write down all systems in less than six units which have moduli in more than one idempotent unit. Tables of such systems have been given by SCHEFFERS,† and in part by STUDY ‡ and ROHR. § As an illustration of the method let us derive all systems in five units with two idempotent units. This case is selected because it is the only one in the least complicated.

By the tables on pages 316 and 318 we see that the following six systems embrace all the irreducible, inequivalent, non-reciprocal systems in question. The group of the nilpotent units e_k ($k = 1, 2, 3$) with respect to e_4 or e_5 is found in the row of e_k and the column of e_4 or e_5.

* The fact here stated is proved in substantially the same manner by SCHEFFERS, loc. cit., page 306.

† Mathematische Annalen, vol. 39.

‡ Göttinger Nachrichten, 1889.

§ Dissertation, loc. cit.

	1		2		3		4		5		6	
	e_4	e_5	e_4	e_5	e_4	e_5	e_4	e_5	e_4	e_5	e_4	e_5
e_1	II	III	II	III	IV	I	II	III	II	III	II	III
e_2	IV	I	II	III	II	III	I	IV	II	III	II	III
e_3	IV	I	IV	I	III	II	IV	I	II	III	III	II

1. By the associative law on the products $e_1e_3^k$ and $e_1e_2^l$ and by theorem IX we see that $e_1e_3 = e_1e_2 = 0$. The sub-systems formed by e_2e_3 must be nilpotent systems in two units, and hence must be in one of the forms given in the tables below (pages 327 and 328 for $n = 2$). (The Roman numerals with subscripts indicate the respectively equivalent systems in SCHEFFERS' classification.)

TABLE 1_1 (V_2)

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	e_1
e_2	0	0	0	0	e_2
e_3	0	0	e_2	0	e_3
e_4	e_1	0	0	e_4	0
e_5	0	e_2	e_3	0	e_5

TABLE 1_2 (V_{14})

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	e_1
e_2	0	0	0	0	e_2
e_3	0	0	0	0	e_3
e_4	e_1	0	0	e_4	0
e_5	0	e_2	e_3	0	e_5

2. From the above general table we have immediately the table following.

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	$a_{13}e_1 + b_{13}e_2$	0	e_1
e_2	0	0	$a_{23}e_1 + b_{23}e_2$	0	e_2
e_3	0	0	$e_3e_3 + f_3e_5$	0	e_3
e_4	e_1	e_2	0	e_4	0
e_5	0	0	e_3	0	e_5

By the transformation $e_3' = e_3 + i\sqrt{f_3}e_5$, f_3' vanishes, and since we can have only two independent idempotent numbers $c_3 = 0$.

Two cases arise:

2_1) $\qquad b_{13} = 0$;

2_2) $\qquad b_{13} \neq 0$.

2_1. By the associative law on $e_1e_3^2$ and $e_2e_3^2$ we get $a_{13} = b_{23} = 0$. We have then the two following systems according as $a_{23} \neq 0$ or $a_{23} = 0$.

TABLE 2_{11} (V_{10})

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	e_1
e_2	0	0	e_1	0	e_2
e_3	0	0	0	0	e_3
e_4	e_1	e_2	0	e_4	0
e_5	0	0	e_3	0	e_5

TABLE 2_{12} (V_{11})

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	e_1
e_2	0	0	0	0	e_2
e_3	0	0	0	0	e_3
e_4	e_1	e_2	0	e_4	0
e_5	0	0	e_3	0	e_5

2_2. If $b_{13} \neq 0$ we transform by

$$e_1' = e_2 + \frac{a_{13}}{b_{13}} e_1$$
$$e_2' = e_1,$$

use the associative law as before and arrive at table 2_{11}.

3. We have immediately from the general table and theorem IX this table:

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	$c_{13}e_3$	0	e_1
e_2	$b_{21}e_2$	0	$d_{23}e_4$	0	e_2
e_3	0	$a_{32}e_1 + f_{32}e_5$	0	e_3	0
e_4	0	e_2	0	e_4	0
e_5	e_1	0	e_3	0	e_5

By the associative law on $e_1^2e_3 = 0$ and $e_2e_1^2 = 0$ we get $c_{13} = b_{21} = 0$. From the product $e_2e_3e_2$ we see that $f_{32} = d_{23}$, and its product $e_3e_2e_1$ shows that $f_{32} = 0$.

Thus we get tables 3_1 and 3_2 according as $a_{23} \neq 0$ or $a_{23} = 0$.

TABLE 3_1 (V_{12})

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	e_1
e_2	0	0	0	0	e_2
e_3	0	e_1	0	e_3	0
e_4	0	e_2	0	e_4	0
e_5	e_1	0	e_3	0	e_5

TABLE 3_2 (V_{13})

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	e_1
e_2	0	0	0	0	e_2
e_3	0	0	0	e_3	0
e_4	0	e_2	0	e_4	0
e_5	e_1	0	e_3	0	e_5

4. From the table on p. 324, theorem IX and by use of the associative law on the products $e_1 e_3^2$ and $e_2^2 e_1$ we have the table 4.

5. Table 5 comes immediately from the table on p. 324.

TABLE 4 (V_3)

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	e_1
e_2	0	0	0	e_2	0
e_3	0	0	0	0	e_3
e_4	e_1	e_2	0	e_4	0
e_5	0	0	e_3	0	e_5

TABLE 5 (V_{30})

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	e_1
e_2	0	0	0	0	e_2
e_3	0	0	0	0	e_3
e_4	e_1	e_2	e_3	e_4	0
e_5	0	0	0	0	e_5

6. From the table on p. 324, by use of the associative law on the products $e_1 e_3 e_1$, $e_2 e_3 e_2$ and $e_1 e_3 e_2$ we get the table 6.

TABLE 6 (V_{31})

	e_1	e_2	e_3	e_4	e_5
e_1	0	0	0	0	e_1
e_2	0	0	0	0	e_2
e_3	0	0	0	e_3	0
e_4	e_1	e_2	0	e_4	0
e_5	0	0	e_3	0	e_5

II.

NILPOTENT SYSTEMS.

In order to derive all systems with a modulus in one idempotent unit it is convenient to prove certain theorems regarding nilpotent systems and their relation to the desired systems.

It is plain from theorem IX *that if any system in n units with a modulus with one idempotent unit is deleted by the modulus, a nilpotent system in* $n-1$ *units remains. If we border a nilpotent system on the right and below with a unit* e_n *such that* $e_k e_n = e_n e_k = e_k (k = 1, \cdots, n)$ *we have a system in group* I *with modulus* e_n.

Def. 16. We call the idempotent and nilpotent systems bearing the above relation to each other *corresponding* systems.

THEOREM XI. *The necessary and sufficient condition that two systems in n units with moduli in one idempotent unit are equivalent is that their corresponding nilpotent systems are equivalent.*

(*a*) If two idempotent systems are equivalent their corresponding systems are equivalent. Let I and I' be idempotent systems with the units $e_1 e_2 \cdots e_n$ and $e'_1 e'_2 \cdots e'_n$ respectively. Let the equations of transformation be

$$e'_k = \sum_{i=1}^{n} a_{ki} e_i \qquad (k = 1, \cdots, n\,;\ |a_{ki}| \neq 0).$$

The equation

$$e'_n = \sum_{i=1}^{n} a_{ni} e_i,$$

must reduce to $e'_n = e_n$ or else we should have two independent idempotent units in I. The remaining equations have $a_{kn} = 0$, otherwise the units $e'_1, e'_2, \cdots, e'_{n-1}$ would not be nilpotent. Thus the equations of transformation become

$$e'_k = \sum_{i=1}^{n-1} a_{ki} e_i, \quad e'_n = e_n \qquad (k = 1, \cdots, n-1\,;\ |a_{ik}| \neq 0)$$

and the condition is necessary.

(*b*) The condition is plainly sufficient, for if we adjoin to the equations which connect the two nilpotent systems in $n - 1$ units the equation $e'_n = e_n$, we have a set of transformations connecting I and I'.

Def. 17.* The *degree of a nilpotent system* is the same as that of the number of highest degree in that system.

By the same method as used in theorem X we see that nilpotent systems of different degrees are inequivalent.

General forms of nilpotent tables.

Degree n.

We have $e_n^n \neq 0$, $e_n^{n+1} = 0$. Then by theorem VIII we have the table

	e_1	e_2	e_3	$\cdots$	e_{n-2}	e_{n-1}	e_n
e_1	0	0	0	$\cdots$	0	0	0
e_2	0	0	0	$\cdots$	0	0	e_1
e_3	0	0	0	$\cdots$	0	e_1	e_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$
e_{n-2}	0	0	0	$\cdots$	e_{n-5}	e_{n-4}	e_{n-3}
e_{n-1}	0	0	e_1	$\cdots$	e_{n-4}	e_{n-3}	e_{n-2}
e_n	0	e_1	e_2	$\cdots$	e_{n-3}	e_{n-2}	e_{n-1}

* PEIRCE, loc. cit., p. 115.

Degree $n-1$.

We have $e_n^{n-1} \neq 0$, $e_n^n = 0$.

By use of the associative law on the product $e_n^n e_1$ and the transformation

$$e_1' = e_1 - \gamma_{n12} e_3 - \gamma_{n13} e_4 - \cdots - \gamma_{n\,1\,n-1} e_n$$

we get

$$e_n e_1 = 0.$$

Hence

$$e_k e_1 = 0 \qquad (k = 2, \cdots, n),$$

since we take the units $e_k = e_n^{n-k+1}$. By the use of the product $e_n e_1 e_n$ we get

$$\gamma_{1n3} = \gamma_{1n4} = \cdots = \gamma_{1nn} = 0.$$

Thus

$$e_1 e_n = \gamma_{1n1} e_1 + \gamma_{1n2} e_2.$$

Similarly using $e_n e_1^2$ we have

$$e_1^2 = \gamma_{111} e_1 + \gamma_{112} e_2.$$

By the use of the product $e_1 e_n^n$ we get $\gamma_{1n1} = 0$, from which we see that $e_1 e_k = 0$ $(k = 2, \cdots, n-1)$. Similarly by $e_1^2 e_2$ we get $\gamma_{111} = 0$. If $\gamma_{112} \neq 0$, $\gamma_{1n2} \neq 0$ we observe by the transformation $e_1' = e_1/\sqrt{\gamma_{112}}$ that $e_1'^2 = e_2$. By the transformation

$$(11) \qquad e_1' = \gamma_{1n2}^{\frac{n-1}{n-3}} e_1, \qquad e_{n-k}' = \gamma_{1n2}^{\frac{2(k+1)}{n-3}} e_{n-k} \qquad (k = 0, 1, \cdots, n-2),$$

we get

$$e_1' e_n' = e_2, \quad e_1' e_k' = 0 \qquad (k = 2, \cdots, n-1),$$

while $e_1'^2 = e_2$. If $\gamma_{112} = 0$ we easily transform the system so that $\gamma_{1n2} = 1$ if it does not vanish, and vice versa. It is necessary to note that transformations (11) fail when $n = 3$, so that a special investigation must be made when deriving systems in three units.

The following table gives the four possible systems of degree $n-1$.

	e_1	e_2	e_3	e_4	$\cdots$	e_{n-1}	e_n
e_1	0 or e_2	0	0	0	$\cdots$	0	0 or e_2
e_2	0	0	0	0	$\cdots$	0	0
e_3	0	0	0	0	$\cdots$	0	e_2
e_4	0	0	0	0	$\cdots$	e_2	e_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
e_{n-1}	0	0	0	e_2	$\cdots$	e_{n-3}	e_{n-2}
e_n	0	0	e_2	e_3	$\cdots$	e_{n-2}	e_{n-1}

Degree $n-2$.

We have $e_n^{n-2} \neq 0$, $e_n^{n-1} = 0$. Thus

$$e_{n-j}e_{n-k} = e_{n-(j+k+1)}^{*} \qquad (j+k+1<n-2),$$

$$e_{n-j}e_{n-k} = 0^{*} \qquad (j,\ k<n-2;\ j+k+1\geqq n-2).$$

If $\gamma_{n21} \neq 0$ we may transform so that $e_n e_2 = e_1$.* If $\gamma_{n21} = 0$ we easily get $e_n e_2 = 0$. In either case $e_n e_1 = 0$.* Thus

$$e_k e_2 = e_k e_1 = 0^{*} \qquad (k = n-1, \cdots, 3).$$

(*Case* 1°) $$e_n e_2 = e_1.$$

By the associative law on the products $e_n e_1 e_n$ and $e_1 e_n^{n-2}$ we get

$$e_1 e_n = \gamma_{1n3} e_3.^{*}$$

Thus

$$e_1 e_{n-k} = 0^{*} \qquad (k = 1, \cdots, n-3).$$

By the product $e_1 e_n e_2$ we get $e_1^2 = 0$.* By the products $e_n e_1 e_2$, $e_n e_2^2$ and e_2^k $(e_2^k = 0)$ we get

$$e_2^2 = \gamma_{221}e_1 + \gamma_{223}e_3 + \gamma_{224}e_4.$$

By the product $e_2^3 = 0$ we see that if $n = 4$, $\gamma_{221}\gamma_{123} = 0$* and $\gamma_{224} = 0$. By $e_n e_2^2$ we get

$$e_1 e_2 = \gamma_{224} e_3.^{*}$$

Similarly

$$e_2 e_1 = \gamma_{213} e_3.^{*}$$

By $e_n e_2 e_n$ we have

$$e_2 e_n = \gamma_{2n1}e_1 + \gamma_{2n3}e_3 + \gamma_{1n3}e_4,^{*}$$

and

$$e_2 e_{n-1} = \gamma_{1n3}(\gamma_{2n1}+1)e_3.^{*}$$

Thus

$$e_2 e_{n-k} = 0^{*} \qquad (k = 2, \cdots, n-3).$$

For $n = 4$ by $e_2 e_n e_2$ we get $\gamma_{213} = \gamma_{1n3} = 0$. For any n we find $\gamma_{213} = \gamma_{2n1}\gamma_{123}$. Thus we have the following table.

	e_1	e_2	e_3	e_4	$\cdots$	e_{n-2}	e_{n-1}	e_n
e_1	0	$\gamma_{224}e_3$	0	0	$\cdots$	0	0	$\gamma_{1n3}e_3$
e_2	$\gamma_{213}e_3$	$\gamma_{221}e_1 + \gamma_{223}e_3 + \gamma_{224}e_4$	0	0	$\cdots$	0	$\gamma_{1n3}(\gamma_{2n1}+1)e_3$	$\gamma_{2n1}e_1 + \gamma_{2n3}e_3 + \gamma_{1n3}e_4$
e_3	0	0	0	0	$\cdots$	0	0	0
e_4	0	0	0	0	$\cdots$	0	0	e_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$	$\vdots$
e_{n-2}	0	0	0	0	$\cdots$	e_{n-5}	e_{n-4}	e_{n-3}
e_{n-1}	0	0	0	0	$\cdots$	e_{n-4}	e_{n-3}	e_{n-2}
e_n	0	e_1	0	e_3	$\cdots$	e_{n-3}	e_{n-2}	e_{n-1}

* Results to be used directly in the table following are marked with an asterisk.

(*Case* 2°) $$e_n e_2 = 0 .$$

In this case by evident use of the associative law we get

$$e_{n-k} e_1 = e_{n-k} e_2 = 0 \qquad (k = 0, \cdots, n-3) ,$$

$$e_i e_k = \sum_{s=1}^{3} \gamma_{iks} e_s \qquad (i = 1, 2; \; k = 1, \cdots, n) .$$

Degree 1.*

Since the square of every number vanishes, if a and β be any two numbers by developing $(a + \beta)^2$ we see that $a\beta = -\beta a$.

From these general tables by considering the various values that the constants in our tables may assume, after some reductions which it is not necessary to reproduce here, we find all the systems desired, the tables so obtained being identical with those in one idempotent unit enumerated by SCHEFFERS, loc. cit., p. 355 ff.

YALE UNIVERSITY, NEW HAVEN, CONN.

* PEIRCE, loc. cit., p. 117.

ON METABELIAN GROUPS

BY

WILLIAM BENJAMIN FITE

Introduction.

The concept of an isomorphism between two groups was introduced by JORDAN in 1868. In the Comptes Rendus of that year, vol. 66, p. 836, he defined an α, 1 isomorphism. Ten years later this concept was generalized to that of an α, β isomorphism by CAPELLI in the Giornali di Matematiche, vol. 16, 1878, p. 33.

Every simple isomorphism of a group with itself may be looked upon as a substitution that replaces each operator of the group by the operator that corresponds to it in this isomorphism. It was first observed by HÖLDER† and MOORE‡ that the totality of these substitutions forms a group. This group is called the group of isomorphisms of the given group.

An isomorphism of a group with itself produced by making every operator of G correspond to its transform with respect to some operator of G is called a cogredient isomorphism. To the totality of cogredient isomorphisms of G corresponds an invariant subgroup of the group of isomorphisms of G. This subgroup is called the group of cogredient isomorphisms of G.§

We define a *Metabelian Group* as *a group whose group of cogredient isomorphisms is abelian.*

The group of cogredient isomorphisms of a group G is simply isomorphic with the quotient group of G with respect to the subgroup formed by the invariant operators of G.‖ If G is metabelian this quotient group is abelian, and therefore the commutators¶ of G are invariant. Conversely, if the commutators of G are invariant, G is metabelian.** Hence we could define a metabelian group as *a group whose commutators are invariant.*

---

* Presented to the Society August 25, December 28, 1899, and February 23, 1901, under various titles. Received for publication February 3, 1902.

† HÖLDER, Mathematische Annalen, vol. 43 (1893), p. 314.

‡ MOORE, Bulletin of the American Mathematical Society, vol. 1 (1894), p. 61.

§ HÖLDER, loc. cit., p. 314.

‖ This is given implicitly by HÖLDER, loc. cit., pp. 329, 330.

¶ DEDEKIND, Mathematische Annalen, vol. 48 (1897), p. 553.

** MILLER, Bulletin of the American Mathematical Society, vol. 4 (1898), pp. 137, 135.

It follows from the definition that every subgroup (and likewise every quotient group) of a metabelian group is either metabelian or abelian.

Let G' be the group of cogredient isomorphisms of a group G, and G'' that of G', and so on. † Then if the series G, G', G'', $\cdots$ ends with identity, G is the direct product of groups of orders $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_n^{\alpha_n}$ respectively, where $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ is the order of G and p_1, p_2, $\cdots$, p_n are distinct primes ‡. Conversely, if G is the direct product of groups of orders $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_n^{\alpha_n}$ respectively, it is evident that we shall arrive at identity by forming these successive groups of cogredient isomorphisms. § In particular, a metabelian group of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ is the direct product of groups of orders $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_n^{\alpha_n}$ respectively.

We shall designate by G' the group of cogredient isomorphisms of the group G. Whenever we speak of the operators of G corresponding to the operators of G' we shall suppose that G and G' are arranged in an $\alpha, 1$ isomorphism, the α invariant operators of G corresponding to identity of G'.

A brief summary of the different sections follows.

In section 1 it is shown that certain abelian groups cannot be groups of cogredient isomorphisms. In addition, some limitations on the order of the group of cogredient isomorphisms under certain conditions are given, together with some theorems on the order of the operators of the group of cogredient isomorphisms. There is also a theorem on the order of an abelian subgroup that is always contained in a metabelian group of order p^m, where p is a prime.

The question of the order of the product of two operators of a metabelian group is considered in section 2.

In the second edition of his *Algebra*, vol. 2, p. 133, Weber states, without proof, that the product of two commutators is not necessarily a commutator. It is the object of section 3 to show that there are certain metabelian groups whose commutator subgroups contain operators that are not commutators.

The number of metabelian groups whose order is a given power of a prime and whose invariant operators form cyclic groups is determined in section 4. It is shown that this number depends only on the different orders of the independent generators of the groups of cogredient isomorphisms and is independent of the number of these generators.

In section 5 a similar, but somewhat more limited, investigation is made concerning metabelian groups whose order is a given power of a prime and whose invariant operators form a subgroup that is the direct product of two cyclic groups of unequal orders, the commutator subgroup being contained in that one of these cyclic subgroups which is of the greater order.

† Cf. AHRENS, Leipziger Berichte, Mathematische-Physiche Klasse, vol. 49 (1897), pp. 616–626.

‡ BURNSIDE, *Theory of Groups of Finite Order*, 1897, p. 115.

§ LOEWY, Mathematische Annalen, vol. 55 (1901), pp. 68, 69.

Section 6 contains a discussion of groups that have metabelian groups of cogredient isomorphisms. It is shown that there are certain metabelian groups that cannot be groups of cogredient isomorphisms. Some of the theorems of this section are similar to those of section 1. An application of the results of this section is made to groups of orders p^5 and p^6, where p is a prime.

I am indebted to Professor Miller for helpful suggestions and criticisms in the preparation of this paper.

§ 1. *Abelian groups of cogredient isomorphisms.*

It is known that G' cannot be cyclic nor the direct product of two cyclic groups of different orders, and that if it is abelian it has no operator of order greater than the order of the subgroup formed by the invariant operators of G.*

Let H denote the subgroup formed by the invariant operators of G. Suppose that G' is abelian with the independent generators $A_1', A_2', \cdots$ of orders $a_1', a_2', \cdots$ respectively. Let $A_1, A_2, \cdots$ be operators of G that correspond respectively to $A_1', A_2', \cdots$. Since G' is abelian, we have

$$A_j^{-1} A_1 A_j = h_j A_1 \qquad (j = 2, 3, \cdots),$$

where the h_j are operators of H. From this we get

$$A_i^{-1} A_1^{a_j'} A_j = h_j^{a_j'} A_1^{a_j'} = A_1^{a_j'}.$$

If now G is of order p^m, where p is a prime, and we denote by a_n' the greatest of the orders $a_2', a_3', \cdots$, then $A_1^{a_n'}$ is commutative with every operator of G and is accordingly contained in H. But this is possible only if a_1' is equal to, or less than, a_n'. Therefore if G is metabelian of order p^m, G' must have at least two independent generators of the highest order.

Now a metabelian group G of order $p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, where $p_1, p_2, \cdots, p_n$ are distinct primes, is the direct product of groups of orders $p_1^{a_1}, p_2^{a_2}, \cdots, p_n^{a_n}$ respectively (see introduction), and G' is the direct product of the groups of cogredient isomorphisms of the respective factor groups.† Let $A_1', A_2', \cdots, A_n'$ be operators of the highest order in the groups of cogredient isomorphisms of the respective factor groups. Let these highest orders be $p_1^{a_1'}, p_2^{a_2'}, \cdots, p_n^{a_n'}$ respectively. From what has just been proved it follows that there are operators $B_1', B_2', \cdots, B_n'$ in these groups of cogredient isomorphisms of orders

$$p_1^{a_1'}, p_2^{a_2'}, \cdots, p_n^{a_n'}$$

respectively that are independent of $A_1', A_2', \cdots, A_n'$. Therefore

$$A_1' A_2' \cdots A_n' \quad \text{and} \quad B_1' B_2' \cdots B_n'$$

* MILLER, Comptes Rendus de l'Académie des Sciences, vol. 128 (1899), p. 229.

† MILLER, Bulletin of the American Mathematical Society, vol. 5 (1899), p. 294.

are two independent generators of G' of the highest order $p_1^{\alpha_1'} p_2^{\alpha_2'} \cdots p_n^{\alpha_n'}$, and the order of every other independent generator of G' is a divisor of $p_1^{\alpha_1'} p_2^{\alpha_2'} \cdots p_n^{\alpha_n'}$. We have proved therefore

THEOREM I.—*The group of cogredient isomorphisms of a group G cannot be the direct product of cyclic groups whose orders are such that any one of them is not a divisor of at least one of the others.*

Now a_1' is the least common multiple of the orders of $h_2, h_3, \cdots$. But these operators (the commutators formed by A_1 and all the operators of G) form an abelian group, and in any abelian group the least common multiple of the orders of any operators is the order of some operator.* Therefore a_1' is the order of a commutator of G. This result can be stated as follows:

THEOREM II.—*The order of every operator of the group of cogredient isomorphisms of a metabelian group G is the order of a commutator of G.*

If G' is abelian the order of H is divisible by every prime factor of the order of G, and therefore if the order of G were not divisible by the cube of a prime, G' would be cyclic. Hence, *no group whose order is not divisible by the cube of a prime can be metabelian.*

The least common multiple of the orders of any operators of a group G that is the direct product of groups whose orders are respectively powers of distinct primes is the order of some operator of G.† In particular, this is true of metabelian groups.

THEOREM III.—*If G is a metabelian group of order g and contains an abelian subgroup of order $g/p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where $p_1, p_2, \cdots, p_n$ are distinct primes, the order of every operator of G' is a divisor of $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$.*

For, let G_1 denote the abelian subgroup of G of order $g/p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and G_1' the subgroup of G' that corresponds to G_1. It may be assumed that G_1 contains H. If A_1 is any operator of G_1 that is not contained in H, it is commutative with at least $g/p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ operators of G and therefore the number of its conjugates in G is a divisor of $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$. The number of commutators of G formed by A_1 and all the operators of G is therefore a divisor of $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$. These commutators form a group. Therefore the order of the operator of G_1' that corresponds to A_1, that is, the order of any operator of G_1', is a divisor of $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$.

If A_2 is any operator of G that is not contained in G_1, then some power of A_2 of the form

$$A_2^{p_1^{\alpha_1'} p_2^{\alpha_2'} \cdots p_n^{\alpha_n'}},$$

where $\alpha_1' \equiv \alpha_1, \alpha_2' \equiv \alpha_2, \cdots, \alpha_n' \equiv \alpha_n$, is contained in G_1, since G_1, whose order is $g/p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, and A_2 generate a subgroup of G. But if

* FROBENIUS and STICKELBERGER, Crelle's Journal, vol. 86 (1879), p. 234.

† The proof of this is similar to that given by FROBENIUS and STICKELBERGER, loc. cit., for abelian groups.

$$A_2^{p_1^{\alpha_1'} p_2^{\alpha_2'} \cdots p_n^{\alpha_n'}} = A_1$$

then A_1 is commutative with at least $g/p_1^{\alpha_1-\alpha_1'} p_2^{\alpha_2-\alpha_2'} \cdots p_n^{\alpha_n-\alpha_n'}$ operators of G and the number of its conjugates in G is a divisor of $p_1^{\alpha_1-\alpha_1'} p_2^{\alpha_2-\alpha_2'} \cdots p_n^{\alpha_n-\alpha_n'}$. The order of the corresponding operator of G' is therefore a divisor of

$$p_1^{\alpha_1-\alpha_1'} p_2^{\alpha_2-\alpha_2'} \cdots p_n^{\alpha_n-\alpha_n'}.$$

Hence the order of every operator of G' is a divisor of $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, and the theorem is proved.

If G_1 is a maximum abelian subgroup of G, the order of G_1' is divisible by $p_1 p_2 \cdots p_n$ and contains no other prime factors besides $p_1, p_2, \cdots, p_n$. If now the order of G_1 is $g/p_1 p_2 \cdots p_n$, G' has an operator of order $p_1 p_2 \cdots p_n$ that is not in G_1' and that with G_1' generates G'. If A_3 is an operator of G that corresponds to this operator of G', A_3 is not commutative with any operator of G_1 that is not in H. The commutators formed by A_3 and two operators A_1 and A_2 of G_1 that correspond to different operators of G_1' are distinct. The number of commutators of G is therefore equal to the order of G_1'. If the order of G is $g = g_1 p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where g_1 is not divisible by $p_1, p_2, \cdots, p_n$, and if G' is of order $p_1^{\alpha_1'} p_2^{\alpha_2'} \cdots p_n^{\alpha_n'}$, then the number of commutators of G is

$$p_1^{\alpha_1'-1} p_2^{\alpha_2'-1} \cdots p_n^{\alpha_n'-1}.$$

The order of H is $g_1 p_1^{\alpha_1-\alpha_1'} p_2^{\alpha_2-\alpha_2'} \cdots p_n^{\alpha_n-\alpha_n'}$. Therefore

$$\alpha_i - \alpha_i' \equiv \alpha_i' - 1; \qquad \alpha_i' \equiv \tfrac{1}{2}(\alpha_i + 1) \qquad (i = 1, 2, \cdots, n).$$

We have therefore

THEOREM IV.—*If G is a metabelian group of order $g = g_1 p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where $p_1, p_2, \cdots, p_n$ are distinct primes and g_1 is not divisible by $p_1, p_2, \cdots, p_n$, and if G has a maximum abelian subgroup of order $g/p_1 p_2 \cdots p_n$, then G' is of order $p_1^{\alpha_1'} p_2^{\alpha_2'} \cdots p_n^{\alpha_n'}$, where*

$$1 < \alpha_i' \equiv \tfrac{1}{2}(\alpha_i + 1) \qquad (i = 1, 2, \cdots, n).$$

Suppose that G has a maximum abelian subgroup of order

$$g_1 p_1^{\alpha_1-\alpha_1'} p_2^{\alpha_2-\alpha_2'} \cdots p_n^{\alpha_n-\alpha_n'}$$

and that G' is of order $p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_n^{\alpha_n-1}$. Consider the subgroup P' of G' of order $p_i^{\alpha_i-1}$ $(i = 1, 2, \cdots, n)$. Let P_1' be the subgroup of P' that is contained in G_1'. Now if any operator of G that corresponds to an operator of P_1' is commutative with every operator of G that corresponds to an operator of P' it is contained in H. Also, an operator of G that corresponds to an operator of P' not in P_1' cannot be commutative with every operator of G that corresponds to an operator of P_1'. Now P_1', considered as a substitution group on the operators of the subgroup of G that corresponds to P', is of degree

$$g_1p_1p_2\cdots p_i^{\alpha_i}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'}\cdots p_n$$

and has

$$g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'-1}\cdots p_n$$

systems of intransitivity. The total number of letters in P_1' (considered as a substitution group) is therefore *

$$p_i^{\alpha_i-\alpha_i'-1}(g_1p_1p_2\cdots p_i^{\alpha_i}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n + g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'-1}\cdots p_n).$$

Now any operator of G that corresponds to an operator of P_1' has p_i conjugates and is commutative with $g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n$ operators of that subgroup of G that corresponds to P'. Therefore the total number of letters in P_1' is

$$(p_i^{\alpha_i-\alpha_i'-1}-1)(g_1p_1p_2\cdots p_i^{\alpha_i}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n),$$

and we have

$$p_i^{\alpha_i-\alpha_i'-1}(g_1p_1p_2\cdots p_i^{\alpha_i}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n + g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'-1}\cdots p_n)$$
$$= (p_i^{\alpha_i-\alpha_i'-1}-1)(g_1p_1p_2\cdots p_i^{\alpha_i}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n).$$

Therefore

$$\alpha_i' = \tfrac{1}{2}(\alpha_i - 1).$$

Hence:

THEOREM V. *If G is a metabelian group of order $g = g_1p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, where $p_1, p_2, \cdots, p_n$ are distinct primes and g_1 is not divisible by $p_1, p_2, \cdots, p_n$, and if G has a maximum abelian subgroup of order $g_1p_1^{\alpha_1-\alpha_1'}p_2^{\alpha_2-\alpha_2'}\cdots p_n^{\alpha_n-\alpha_n'}$, its group of cogredient isomorphisms cannot be of order $p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_n^{\alpha_n-1}$ unless $\alpha_i' = \frac{1}{2}(\alpha_i - 1)$ $(i = 1, 2, \cdots, n)$.*

If G is any group of order p^m, where p is a prime, it is known that it has an abelian subgroup of order p^γ, if

$$\frac{\gamma(\gamma-1)}{2} < m.\dagger$$

If now G is a metabelian group, the minimum value of m in order that G necessarily contain an abelian subgroup of order p^γ is less than this value when $\gamma > 3$, as is shown in the following

THEOREM VI.—*If G is a metabelian group of order p^m, where p is a prime it contains an abelian subgroup of order p^γ if*

$$m > \frac{(\gamma+3)(\gamma-1)}{4}.$$

*FROBENIUS, Crelle's Journal, vol. 101 (1887), p. 287.

†MILLER, Messenger of Mathematics, vol. 27 (1897-8), p. 120.

Suppose that G contains p^α invariant operators and that its commutator subgroup is of order p^β. Let A_1 be a non-invariant operator of G. It has no more than p^β conjugates and is therefore invariant in a G_1 of order $p^{m-\beta}$ that has at least $p^{\alpha+1}$ invariant operators. Any non-invariant operator A_2 of G_1 is invariant in a G_2 of order $p^{m-2\beta}$ that has at least $p^{\alpha+2}$ invariant operators. By continuing this process, we see that $G_{\gamma-\alpha-1}$ of order $p^{m-(\gamma-\alpha-1)\beta}$ contains $p^{\gamma-1}$ invariant operators, if $m-(\gamma-\alpha-1)\beta > \gamma-1$. In this case $G_{\gamma-\alpha-1}$ contains an abelian subgroup of order p^γ. But $m-(\gamma-\alpha-1)\beta > \gamma-1$, if $m > \frac{1}{4}(\gamma+3)(\gamma-1)$, since $\beta \equiv \alpha$.

§ 2. *The order of the product of two operators of a metabelian group.*

Let A and B be any two operators of a metabelian group G, so that

$$A^{-1}BA = hB, \qquad A^{-1}B^xA = h^xB^x,$$

where x is any integer. Then

$$(AB)^x = h^{\frac{1}{2}x(x-1)}A^xB^x.$$

Suppose that A and B are of orders α and β respectively, and let μ be the least common multiple of α and β. Then

$$(AB)^\mu = h^{\frac{1}{2}\mu(\mu-1)}A^\mu B^\mu = h^{\frac{1}{2}\mu(\mu-1)}.$$

Now the order of h is a divisor of both α and β. Therefore if α and β are both odd, or if they contain the factor 2 to different powers,

$$(AB)^\mu = 1.$$

But if α and β contain the factor 2 to the same power, we cannot conclude that

$$(AB)^\mu = 1.$$

In this case, however,

$$(AB)^{2\mu} = 1.$$

The operators $A \equiv bd$, $B \equiv ab\cdot cd\cdot efg$ of the group $(abcd)_8(efg)cyc$ * may be cited as two operators of a metabelian group the order of whose product is twice the least common multiple of their orders.

Let γ be the order of $C = AB$, and let p^a, p^b, p^c be the highest powers of p (any prime) contained in α, β, γ respectively. Then since $BC^{-1} = A^{-1}$ and $C^{-1}A = B^{-1}$, it follows from the preceding that of the numbers a, b, c two are equal and the third one less than, or equal to, the other two, except that in the case $p = 2$ the third one may be one greater than the value of the other two.

Hence:

* For this notation see CAYLEY, Quarterly Journal of Mathematics, vol. 25 (1890-1), p. 76.

THEOREM I.—*If G is a metabelian group, the order γ of the product of any two of its operators A and B of orders α and β respectively must be a divisor of the least common multiple of α and β, except that when α and β contain the same power of 2 as a factor, γ is a divisor of twice the least common multiple of α and β. Also γ must be a multiple of the least common multiple of α' and β', where $\alpha = \delta\alpha'$, $\beta = \delta\beta'$, δ being the product of the powers of all the prime factors that occur to the same power in α and β, except that, when one of the numbers α, β contains the factor 2 to a power one higher than the other one does, γ is a multiple of one-half the least common multiple of α' and β'.*

COROLLARY.—*If α and β are relatively prime, $\alpha\beta$ is the order of AB.*

This follows from the fact that in this case A and B are commutative.

COROLLARY.—*If G is a metabelian group of order p^m, where p is an odd prime, the order of the product of any two of its operators A and B, of orders p^{n_1} and p^{n_2} respectively $(n_1 > n_2)$, is p^{n_1}. If $p = 2$, the order of AB must be 2^{n_1}, except that it may be 2^{n_2} when $n_1 = n_2 + 1$.*

If G is an abelian group, the order of AB is a multiple of the least common multiple of α' and β', and a divisor of the least common multiple of α and β. Two commutative operators A and B can be chosen so that the order of AB is any multiple of the least common multiple of α' and β' that is also a divisor of the least common multiple of α and β. For, take

$$A \equiv a_1 a_2 \cdots a_\delta \cdot b_1 b_2 \cdots b_{\delta'} \cdot c_1 c_2 \cdots c_{\alpha'},$$

where δ' is any divisor of δ, and

$$B \equiv a_\delta a_{\delta-1} \cdots a_2 a_1 \cdot d_1 d_2 \cdots d_{\beta'}.$$

The order of AB is δ' times the least common multiple of α' and β'.

THEOREM II.—*In a metabelian group G the order of the product of two operators that correspond respectively to two independent operators of G' is a multiple of the least common multiple of the orders of these operators of G'.*

This follows from the fact that the order of the product of two independent commutative operators is the least common multiple of the orders of the operators.

THEOREM III.—*In a metabelian group G of order p^m, where p is a prime, the order of the product of two operators that correspond respectively to two operators of G' of different orders is equal to, or greater than, the greater of these orders.*

This follows from the fact that the order of the product of two commutative operators of orders p^{n_1} and p^{n_2} respectively, where $n_1 > n_2$, is p^{n_1}.

THEOREM IV.—*If G is a metabelian group of order p^m, where p is an odd*

prime, the p^β power of all the operators form a group, p^β being the highest order of any commutator of G.

For if $A^{p^\beta} = h_1$, and $B^{p^\beta} = h_2$, then

$$(AB)^{p^\beta} = h^{\frac{1}{2}p^\beta(p^\beta-1)} A^{p^\beta} B^{p^\beta} = h_1 h_2,$$

where $A^{-1}BA = hB$.

§ 3. *The commutators of a metabelian group.*

The commutator subgroup of a group is invariant in the group,* and in a group of order p^m an operator of order p cannot be transformed into one of its own powers, except the first.† Hence, *a group of order p^m, where p is a prime, is metabelian if its commutator subgroup is of order p.*

If the commutator subgroup of a group G of order p^m is of order p^a and contains a subgroup H_1 of order p^{a-1} that is invariant in G, then G/H_1 is met. abelian, since its commutator subgroup is of order p.

Let G be a metabelian group whose group of cogredient isomorphisms is generated by three independent operators. Let A_1, A_2, A_3 be three operators of G that correspond respectively to the three generators A_1', A_2', A_3', of G'. If

$$A_2^{-1}A_1A_2 = h_1A_1, \qquad A_3^{-1}A_1A_3 = h_2A_1, \qquad A_3^{-1}A_2A_3 = h_3A_2,$$

then h_1, h_2, h_3 generate the commutator subgroup of G. We proceed to prove that every operator of this subgroup is a commutator.

This is done by showing that integral values of a_1, a_2, a_3, b_1, b_2, b_3 can be found that will satisfy the relation

$$(A_1^{a_1}A_2^{a_2}A_3^{a_3})^{-1} \cdot A_1^{b_1}A_2^{b_2}A_3^{b_3} \cdot (A_1^{a_1}A_2^{a_2}A_3^{a_3}) = h_1^{a_1}h_2^{a_2}h_3^{a_3}A_1^{b_1}A_2^{b_2}A_3^{b_3}$$

for all integral values of α_1, α_2, α_3 taken modulo the orders of h_1, h_2, h_3 respectively.

Now

$$(A_1^{a_1}A_2^{a_2}A_3^{a_3})^{-1} \cdot A_1^{b_1}A_2^{b_2}A_3^{b_3} \cdot (A_1^{a_1}A_2^{a_2}A_3^{a_3}) = h_3^{a_3b_2}h_2^{a_3b_1}h_3^{-a_2b_3}h_1^{a_2b_1}h_2^{-a_1b_3}h_1^{-a_1b_2}A_1^{b_1}A_2^{b_2}A_3^{b_3}.$$

Hence the relation given above will be satisfied if the following equations are satisfied

$$a_2b_1 - a_1b_2 = \alpha_1, \qquad a_3b_1 - a_1b_3 = \alpha_2, \qquad a_3b_2 - a_2b_3 = \alpha_3.$$

But integral values of a_1, a_2, a_3, b_1, b_2, b_3 can always be found that satisfy these equations.

* MILLER, Quarterly Journal of Mathematics, vol. 28 (1896), p. 266. Cf. FROBENIUS, Berliner Sitzungsberichte, 1896, p. 1348.

† FROBENIUS, loc. cit., 1895, p. 982.

If h_1, h_2, h_3 are not all distinct, or if any of them equal identity, the conclusion still holds.

Consider now a metabelian group G of order p^m whose group of cogredient isomorphisms is generated by four independent operators, A_1', A_2', A_3', A_4', and let A_1, A_2, A_3, A_4 be operators of G that correspond respectively to these generators of G'. Let

$$A_2^{-1}A_1A_2 = h_1A_1, \qquad A_3^{-1}A_1A_3 = h_2A_1, \qquad A_4^{-1}A_1A_4 = h_3A_1,$$
$$A_3^{-1}A_2A_3 = h_4A_2, \qquad A_4^{-1}A_2A_4 = h_5A_2, \qquad A_4^{-1}A_3A_4 = h_6A_3.$$

We assume that it is possible that the h_i $(i = 1, 2, \cdots, 6)$ be all different from identity and independent. We shall justify this assumption later.

Now the h_i $(i = 1, 2, \cdots, 6)$ generate the commutator subgroup of G; that is, every commutator is obtained from $A_1^{a_1}A_2^{a_2}A_3^{a_3}A_4^{a_4}$ and $A_1^{b_1}A_2^{b_2}A_3^{b_3}A_4^{b_4}$, where a_1, a_2, a_3, a_4, and also b_1, b_2, b_3, b_4 take all possible values modulo the orders of A_1', A_2', A_3', A_4' respectively.

We have

$$(A_1^{a_1}A_2^{a_2}A_3^{a_3}A_4^{a_4})^{-1}A_1^{b_1}A_2^{b_2}A_3^{b_3}A_4^{b_4}(A_1^{a_1}A_2^{a_2}A_3^{a_3}A_4^{a_4})$$
$$= h_1^{a_2b_1-a_1b_2}h_2^{a_3b_1-a_1b_3}h_3^{a_4b_1-a_1b_4}h_4^{a_3b_2-a_2b_3}h_5^{a_4b_2-a_2b_4}h_6^{a_4b_3-a_3b_4}A_1^{b_1}A_2^{b_2}A_3^{b_3}A_4^{b_4}.$$

If now p^{m_i} is the order of h_i, and k_i is an integer $(i = 1, 2, \cdots, 6)$, then $h_1^{\alpha_1}h_2^{\alpha_2}h_3^{\alpha_3}h_4^{\alpha_4}h_5^{\alpha_5}h_6^{\alpha_6}$ is an operator of the commutator subgroup of G that is not a commutator if integral values of a_i and b_j $(i, j = 1, 2, \cdots, 4)$ cannot be found to satisfy the following equations:

$$a_2b_1 - a_1b_2 = \alpha_1 + k_1p^{m_1}, \quad a_3b_1 - a_1b_3 = \alpha_2 + k_2p^{m_2}, \quad a_4b_1 - a_1b_4 = \alpha_3 + k_3p^{m_3},$$
$$a_3b_2 - a_2b_3 = \alpha_4 + k_4p^{m_4}, \quad a_4b_2 - a_2b_4 = \alpha_5 + k_5p^{m_5}, \quad a_4b_3 - a_3b_4 = \alpha_6 + k_6p^{m_6}.$$

Such integral values cannot be found to satisfy these equations for all values of α_i $(i = 1, 2, \cdots, 6)$; *e. g.*, for $\alpha_i = 1$. Therefore if a group exists that has the properties assumed, the commutator subgroup of this group contains operators that are not commutators. The group generated by the following operators is such a group: *

$$h_1 \equiv ac \cdot bd, \qquad h_2 \equiv eg \cdot fh, \qquad h_3 \equiv ik \cdot jl,$$
$$h_4 \equiv mo \cdot np, \qquad h_5 \equiv qs \cdot rt, \qquad h_6 \equiv uw \cdot vx,$$
$$A_1 \equiv ac \cdot eg \cdot ik, \qquad A_2 \equiv ab \cdot cd \cdot mo \cdot qs,$$
$$A_3 \equiv ef \cdot gh \cdot mn \cdot op \cdot uw, \qquad A_4 \equiv ij \cdot kl \cdot qr \cdot st \cdot uv \cdot wx.$$

* This group was constructed by Professor MILLER.

The order of this group is 1024. The commutator subgroup is of order 64. It contains 36 commutators and 28 operators that are not commutators.

If $h_5 = h_6 = 1$, that is, if A_4 is commutative with A_2 and A_3, the commutator subgroup is unchanged except that h_5 and h_6 are replaced by identity. Now $h_3 h_4$ is not a commutator in the original group. Moreover no commutator of the original group reduces to $h_3 h_4$ when h_5 and h_6 are replaced by identity. Hence if there is a group with these properties, its commutator subgroup contains operators that are not commutators. Such a group is generated by the following operators:

$$h_1 \equiv ac \cdot bd, \quad h_2 \equiv eg \cdot fh, \quad h_3 \equiv ik \cdot jl, \quad h_4 \equiv mo \cdot np,$$

$$A_1 \equiv ac \cdot eg \cdot ik, \quad A_2 \equiv ab \cdot cd \cdot mo, \quad A_3 \equiv ef \cdot gh \cdot mn \cdot op, \quad A_4 \equiv ij \cdot kl.$$

The order of this group is 256. Its commutator subgroup is of order 16 and contains only 15 commutators.

§ 4. *Metabelian groups whose commutator subgroups are cyclic.*

Let G be a metabelian group of order p^m, where p is a prime. Suppose that the commutator subgroup of G is cyclic of order p^α and that $A_1, A_2, \cdots, A_n$ are operators of G corresponding respectively to the independent generators of G' that are of the highest order p^{α_1}. No one of these, as A_1, can be commutative with all the others, for in that case A_1 would be invariant in the subgroup of G corresponding to the subgroup of G' that is generated by the generators of highest order in G'. Hence no commutator of highest order in G could be formed by A_1 and any operator of G. But such a commutator can always be formed by A_1 and some operator of G.

We may assume therefore that $A_1^{-1} A_2 A_1 = h A_2$, where h is a commutator of G of order p^{α_1}. We can choose for $A_3, A_4, \cdots, A_n$ operators that are commutative with A_1 and A_2. For if $A_1^{-1} A_3 A_1 = h_1 A_3$, h_1 must be a power of h, say $h_1 = h^a$, since the commutator subgroup is cyclic. Now

$$A_1^{-1} \cdot A_2^{p^{\alpha_1 - \alpha}} A_3 \cdot A_1 = A_2^{p^{\alpha_1 - \alpha}} A_3 \equiv B_3,$$

and we can take the operator B_3' of G' that corresponds to B_3 as a generator in place of A_3'. If $A_2^{-1} B_3 A_2 = h_2 B_3$, then $h_2 = h^b$ and

$$A_2^{-1} \cdot A_1^{b - p^{\alpha_1}} B_3 \cdot A_2 = A_1^{b - p^{\alpha_1}} B_3 \equiv C_3.$$

In place of B_3' we can take C_3' as one of the independent generators of G' of order p^{α_1}. Both A_1 and A_2 are commutative with C_3. Similarly, if $A_4, \cdots, A_n$ are not commutative with A_1 and A_2, we can choose in place of them operators that are. Of these we can find two whose commutator is of

order p^{α_1}, and then choose all the others so that they are commutative with these two and with A_1 and A_2. Proceeding in this way, we can arrange the generators of G' of order p^{α_1} in pairs. If there should be an odd number of these generators, an operator of G corresponding to one of them would be commutative with every operator of G that corresponds to an independent generator of G' of order p^{α_1}. It has been shown that this is impossible.

By similar reasoning it can be shown that the independent generators of G' can be so chosen that any operator of G corresponding to an independent generator of G' of any order is commutative with those operators of G that correspond to the independent generators of G' of any higher order, and is not commutative with all the operators of G that correspond to independent generators of G' of the same order. We have therefore

THEOREM I.—*If the commutators of a metabelian group of order p^m, where p is a prime, form a cyclic group, the number of independent generators of any given order of G' is even.**

Consider a metabelian group $G \equiv \{Q, A_1, A_2\}$ whose invariant operators form the cyclic group $\{Q\}$ of order p^α and whose group of cogredient isomorphisms is of order $p^{2\beta}$ of the type (β, β). We can assume that

$$A_1^{p^\beta} = A_2^{p^\beta} = Q^{p^{\beta-i}} \qquad (i = 0, 1, 2, \cdots, \beta).$$

If $i = 0$, the relations

$$A_1^{p^\beta} = A_2^{p^\beta} = 1$$

define the same group as the relations just given.

There are accordingly no more than $\beta + 1$ types of metabelian groups whose invariant operators form a cyclic group of order p^α and whose groups of cogredient isomorphisms are of order $p^{2\beta}$ of the type (β, β). These $\beta + 1$ types may be defined as follows:

$$Q^{p^\alpha} = 1, \qquad A_1^{p^\beta} = A_2^{p^\beta} = Q^{p^{\beta-i}} \qquad (i = 0, 1, 2, \cdots, \beta),$$

$$A_1^{-1} A_2 A_1 = A_2 Q^{p^{\alpha-\beta}}, \qquad A_1 Q = Q A_1, \qquad A_2 Q = Q A_2.$$

These relations in every case define a group, since substitution groups can be constructed that satisfy them. Moreover these groups are distinct.

If G is a metabelian group of order p^m, where p is a prime, whose commutator subgroup is cyclic and whose group of cogredient isomorphisms is of the type $(\beta, \beta, \cdots,$ with $2s$ terms), s being any positive integer, there always exists a metabelian group of order $p^{m+2\beta}$ whose invariant operators are the same as those of G and whose group of cogredient isomorphisms is of the type $(\beta, \beta, \cdots,$ with $2s + 2$ terms). For, if G be represented as a regular substitu-

*Cf. YOUNG, American Journal of Mathematics, vol. 15 (1893), p. 171; BURNSIDE, *Theory of Groups of Finite Order*, 1897, p. 68.

tion group and G_1 is the simply isomorphic group all of whose substitutions are commutative with every substitution of G*, and if A_1 and A_2 are a pair of generators of G such as are described in the preceding discussion, and B_1 and B_2 the corresponding substitutions of G_1, — then $G_2 \equiv \{G, B_1, B_2\}$ is a metabelian group with the same invariant operators and the same commutators that G has, and the group of cogredient isomorphisms of G_2 is of the type $(\beta, \beta, \cdots,$ with $2s+2$ terms). We have just shown that $\beta+1$ metabelian groups exist whose invariant operators form a cyclic group of order p^α, α being any positive integer, and whose groups of cogredient isomorphisms are of the type (β, β), where $\beta \leqq \alpha$. Therefore metabelian groups exist whose invariant operators form a cyclic group of order p^α and whose groups of cogredient isomorphisms are of the type $(\beta, \beta, \cdots$ with $2s$ terms), s being any positive integer.

Let G be such a group, and let A_1, A_2; A_3, A_4 be two pairs of generators such as have been described. If

$$A_1^{p^\beta} = A_2^{p^\beta} = Q^{p^{\beta-i}}, \qquad A_3^{p^\beta} = A_4^{p^\beta} = Q^{p^{\beta-j}} \qquad (j>i),$$

$$A_2^{-1}A_1A_2 = A_1Q^{p^{\alpha-\beta}}, \qquad A_4^{-1}A_3A_4 = A_3Q^{p^{\alpha-\beta}},$$

$$A_1A_3 = A_3A_1, \quad A_1A_4 = A_4A_1, \quad A_2A_3 = A_3A_2, \quad A_2A_4 = A_4A_2,$$

then in place of A_1, A_2, A_3, A_4 we can take the following:

$$B_1 \equiv A_3^{1-p^{j-i}}A_1, \qquad B_2 \equiv A_3^{1-p^{j-i}}A_2, \qquad B_3 \equiv A_3,$$

and, according as p is odd or even,

$$B_4 \equiv A_1^{-p^\beta - p^{j-i}+1}A_2^{p^\beta + p^{j-i}-1}A_4,$$

or

$$B_4 \equiv A_1^{-p^\beta - p^{j-i}+1}A_2^{p^\beta + p^{j-i}-1}A_3^{x}A_4,$$

where

$$x(1+p^{\alpha-\beta+j-1}) \equiv p^{\alpha-\beta+j-i} \pmod{p^{\alpha-\beta+j}}.$$

Either of these pairs generates with $\{Q\}$ a group that is simply isomorphic with $\{Q, A_3, A_4\}$. Also B_1 and B_2 are commutative with B_3 and B_4, and

$$B_2^{-1}B_1B_2 = B_1Q^{p^{\alpha-\beta}}, \qquad B_4^{-1}B_3B_4 = B_3Q^{p^{\alpha-\beta}}.$$

Therefore the subgroups generated by $\{Q\}$ and the respective pairs of generators may be assumed to be all of one type and we have

THEOREM II.—*There are exactly $\beta+1$ groups of order $p^{\alpha+2\beta s}$, where p is a prime, α, β, and s positive integers, and $\beta \leqq \alpha$, whose invariant operators*

*JORDAN, Journal de l'Ecole Polytechnique, vol. 22 (1861), p. 153.

form a cyclic group of order p^α and whose groups of cogredient isomorphisms are abelian of the type

$$(\beta, \beta, \cdots \textit{with } 2s \textit{ terms}).^*$$

Suppose that the invariant operators of a group G form a cyclic group $\{Q\}$ of order p^α, where p is a prime, and that G is abelian of the type

$$(\alpha_1, \alpha_1, \cdots \text{with } 2s_1 \text{ terms};\ \alpha_2, \alpha_2, \cdots \text{with } 2s_2 \text{ terms};\ \cdots;$$
$$\alpha_n, \alpha_n, \cdots, \text{with } 2s_n \text{ terms}),$$

where $\alpha_1 < \alpha_2 < \cdots < \alpha_{n-1} < \alpha_n \equiv \alpha$. We know that there are $\alpha_i + 1$ metabelian groups whose invariant operators form a cyclic group of order p^α and whose groups of cogredient isomorphisms are of the type

$$(\alpha_i, \alpha_i, \cdots \text{with } 2s_i \text{ terms}) \qquad (i = 1, 2, \cdots, n).$$

We shall represent these $\alpha_i + 1$ groups by the symbols

$$G_{0,i}, G_{1,i}, \cdots, G_{\alpha_i, i}.$$

We write down the following scheme in which the groups of the i-th column are the $\alpha_i + 1$ groups whose groups of cogredient isomorphisms are of the type

$$(\alpha_i, \alpha_i, \cdots \text{with } 2s_i \text{ terms}):$$

$$\begin{array}{ccccccccc}
G_{0,1}, & G_{0,2}, & \cdots, & G_{0,i}, & \cdots, & G_{0,n} \\
G_{1,1}, & G_{1,2}, & \cdots, & G_{1,i}, & \cdots, & G_{1,n} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
G_{\alpha_1,1}, & G_{\alpha_1,2}, & \cdots, & G_{\alpha_1,i}, & \cdots, & G_{\alpha_1,n} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
G_{\alpha_2,2}, & \cdots, & G_{\alpha_2,i}, & \cdots, & G_{\alpha_2,n} \\
\cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot \\
G_{\alpha_i,i}, & \cdots, & G_{\alpha_i,n} \\
\cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot \\
G_{\alpha_n,n}.
\end{array}$$

All the groups in this scheme have the same invariant operators, but no two of the groups have any non-invariant operators in common. The groups in the

* This result does not agree with that obtained by BURNSIDE, loc. cit., p. 69. For the case $\beta = 1$, see YOUNG, loc. cit., pp. 168-177.

jth row ($j = 1, 2, \cdots, a_n^{+1}$) contain operators of order p^{a+j-1} but none of higher order.* Any group G whose invariant operators form a cyclic group of order p^a and whose group of cogredient isomorphisms is abelian of the type given above can be generated by groups in this scheme, one group being taken from each column. Any group generated in this way is of the type under consideration. It is assumed that all the operators of any group in any column of this scheme are commutative with all the operators of all the groups contained in all the other columns.

We now consider how many distinct groups can be obtained in this way; that is, how many distinct groups are contained in the scheme

$$\{G_{i_1,1},\ G_{i_2,2},\ \cdots,\ G_{i_n,n}\},$$

where $i_j = 0, 1, 2, \cdots, \alpha_j$, and $j = 1, 2, \cdots, n$.

In the first place, $G_{i,j}$ and $G_{k,l}$, where $k < i$ and $l > j$, generate the same group as $G_{i,j}$ and $G_{i,l}$. For if A is an operator of order p^{a+i} in $G_{i,j}$ corresponding to an independent generator of $G'_{i,j}$ of order p^{a_j}, and B is an operator of order p^{a+k} in $G_{k,l}$ corresponding to an independent generator of $G'_{k,l}$ of order p^{a_l}, then AB is an operator of $\{G_{i,j},\ G_{k,l}\}$ of order p^{a+i} and corresponds to an operator of order p^{a_l} in the group of cogredient isomorphisms of $\{G_{i,j},\ G_{k,l}\}$. This latter may be taken as one of the independent generators of order p^{a_l} of this group of cogredient isomorphisms.

We can take for B in turn operators of order p^{a+k} corresponding respectively to the independent generators of order p^{a_l} of $G'_{k,l}$, and each time we get an operator of $\{G_{i,j},\ G_{k,l}\}$ of order p^{a+i} corresponding to an independent generator of the group of cogredient isomorphisms of $\{G_{i,j},\ G_{k,l}\}$ of order p^{a_l}. Therefore $\{G_{i,j},\ G_{k,l}\} \equiv \{G_{i,j},\ G_{i,l}\}$.

Suppose now that A is an operator of order p^{a+i} in $G_{i,j}$ corresponding to an independent generator of $G'_{i,j}$ of order p^{a_j}, and that B is an operator of order p^{a+i+x} in $G_{i+x,k}$ corresponding to an independent generator of $G'_{i+x,k}$ of order p^{a_k}, where $k > j$. Then $AB^{p^{a_k-a_j}}$ corresponds to an operator of order p^{a_j} in the group of cogredient isomorphisms of $\{G_{i,j},\ G_{i+x,k}\}$. This may be taken as one of the independent generators of order p^{a_j} in this group of cogredient isomorphisms. Now $B^{p^{a_k-a_j}}$ is of order $p^{a+i+x-a_k+a_j}$ and the order of $AB^{p^{a_k-a_j}}$ is $p^{a+i+x-a_k+a_j}$, if $x > \alpha_k - \alpha_j$. It follows, therefore, if $x > \alpha_k - \alpha_j$, that

$$\{G_{i,j},\ G_{i+x,k}\} \equiv \{G_{i+x-(a_k-a_j),j},\ G_{i+x,k}\}.$$

Hence in order to get all the distinct groups in the scheme

$$\{G_{i_1,1},\ G_{i_2,2},\ \cdots,\ G_{i_n,n}\}$$

* If $p = 2$, $G_{0,n}$ contains operators of order p^{a+1}. Some of the statements in the following argument would have to be modified to cover this case, but the final result, as stated in Theorem III, is the same whether p is even or odd.

we need to combine with $G_{i_x,x}$ only $\alpha_{x+1}-\alpha_x+1$ groups of the type $G_{i_{x+1},x+1}$ namely, those for which

$$0 \leqq i_{x+1}-i_x \leqq \alpha_{x+1}-\alpha_x.$$

Therefore the number of distinct groups in the scheme under consideration is equal to, or less than,

$$(\alpha_1+1)(\alpha_2-\alpha_1+1)\cdots(\alpha_n-\alpha_{n-1}+1).$$

Now, these groups are all distinct, since any two must differ in at least one of the components, say that one contains $G_{i,j}$ and that the other contains $G_{i',j}$, where $i'>i$; and the one has no operator of order greater than $p^{\alpha+i}$ corresponding to an independent generator of order p^{α_j} in the group of cogredient isomorphisms, while the other has such an operator of order $p^{\alpha+i'}$.

The relations under consideration always define a group since substitution groups can be constructed that satisfy these relations. We can therefore enunciate the following

THEOREM III.—*The number of metabelian groups whose invariant operators form a cyclic group of order p^α, where p is a prime, and whose groups of cogredient isomorphisms are of order $p^{2(a_1s_1+a_2s_2+\cdots+a_ns_n)}$ of the type*

$(\alpha_1, \alpha_1, \cdots$ *with* $2s_1$ *terms,* $\alpha_2, \alpha_2, \cdots$ *with* $2s_2$ *terms,* $\cdots$,

$\alpha_n, \alpha_n, \ldots$ *with* $2s_n$ *terms*),

where $\alpha_1<\alpha_2<\cdots<\alpha_{n-1}<\alpha_n \leqq \alpha$, *and* $s_1, s_2, \cdots s_n$ *are any positive integers, is*

$$(\alpha_1+1)(\alpha_2-\alpha_1+1)\cdots(\alpha_n-\alpha_{n-1}+1).$$

§ 5. *Metabelian groups whose invariant operators form a group that is the direct product of two cyclic groups.*

We shall now consider the number of metabelian groups of order p^m, p being a prime, whose invariant operators form a subgroup that is the direct product of two cyclic groups of orders p^{α_1} and p^{α_2} respectively, and whose groups of cogredient isomorphisms are of order $p^{2\beta}$ and of type (β, β). It is assumed that

$$\alpha_1-\beta \leqq \alpha_2, \quad \beta \leqq \alpha_2,$$

and that the commutator subgroup is contained in the cyclic subgroup of order p^{α_1} formed by invariant operators.

The subgroup H formed by the invariant operators has the independent generators Q, R, of orders p^{α_1} and p^{α_2} respectively. The entire group G is gen-

erated by H, A, B, where A and B are operators of G corresponding to independent generators of G' of order p^β. We can always choose A and B so that A^{p^β} is contained in $\{Q\}$ and B^{p^β} is not contained in $\{Q\}$, unless $B^{p^\beta} = A^{p^\beta}$. Therefore all the groups under consideration can be represented by the symbol ${}_kG_{i,j}$ $(k = 0, 1, 2, \cdots, \beta;\ i = 0, 1, p, p^2, \cdots, p^{\beta-1};\ j = 0, 1, p, p^2, \cdots, p^{\alpha_2-1})$. The subscript k, at the left, indicates that $A^{p^\beta} = Q^{p^{\beta-k}}$, and the subscripts i, j, at the right indicate that $B^{p^\beta} = Q^i R^j$. If $i > p^{\beta-1}$, we can take

$$B_1 \equiv Q^{-ip^\beta} B$$

for B. Then $B_1^{p^\beta} = R^j$. If $k = 0$, we have $A^{p^\beta} = Q^{p^\beta}$. This gives the group in which $A^{p^\beta} = 1$, since if we take $A_1 \equiv Q^{-1}A$ for A, then $A_1^{p^\beta} = 1$. When $j = 0$, we may take $i = p^{\beta-k}$.

These relations in every case define a group, since substitution groups can be constructed that satisfy them.

We have now to consider how many distinct groups are represented by ${}_kG_{i,j}$. The following identities can be established:

$${}_kG_{i,j} \equiv {}_kG_{0,j}, \qquad \text{when} \qquad p^{\beta-k} \not\equiv i \not\equiv p^{\beta-1}, j > 0;$$

$${}_kG_{i,j} \equiv {}_0G_{i,j}, \qquad \text{when} \qquad \frac{p^{\beta-k}}{i} \not\equiv \frac{p^{\alpha_2}}{j}, i > 0, j > 0;$$

$${}_0G_{p^l,j} \equiv {}_{\beta-l}G_{0,0}, \qquad \text{when} \qquad j \not\equiv p^l;$$

$${}_kG_{i,j} \equiv {}_{k'}G_{0,j'}, \qquad \text{when} \qquad i = p^{\beta-k'},\ j' = \frac{jp^{\beta-k}}{i},\ i \not\equiv j.$$

By considering the orders of their operators it can be shown that those groups are distinct for which the following relations hold:

$$\frac{p^{\beta-k}}{i} < \frac{p^{\alpha_2}}{j}, \qquad \text{when} \qquad i > 0, \quad j > 0, \quad k > 0;$$

$$i < p^{\beta-k}, \qquad \text{when} \qquad j > 0;$$

$$j < i, \qquad \text{when} \qquad i > 0, \quad j > 0;$$

$$i = p^{\beta-k}, \quad k > 0, \quad \text{or} \quad i = k = 0, \quad \text{when} \quad j = 0.$$

It follows from the above that there is no other distinct group ${}_kG_{i,j}$. The number of groups ${}_kG_{i,j}$ satisfying these relations is

$$N = \beta + 1 + \frac{\alpha_2(5 + 3\beta + 3\alpha_2\beta - 2\alpha_2^2)}{6}.$$

We can state this result as follows:

THEOREM I.—There are

$$\beta + 1 + \frac{\alpha_2(5 + 3\beta + 3\alpha_2\beta - 2\alpha_2^2)}{6}$$

metabelian groups of order $p^{\alpha_1+\alpha_2+2\beta}$, *where* p *is a prime,* $\alpha_1 - \beta \equiv \alpha_2$, $\beta \equiv \alpha_2$, *whose groups of cogredient isomorphisms are of order* $p^{2\beta}$ *and of the type* (β, β), *and whose invariant operators form a group that is the direct product of an operator of order* p^{α_1} *and one of order* p^{α_2}, *the commutators being powers of the operator of order* p^{α_1}.

§ 6. *Groups that have metabelian groups of cogredient isomorphisms.*

If we form the group of cogredient isomorphisms G' of any group G, then the group of cogredient isomorphisms G'' of G', and so on, we finally come either to identity or to a group that has no invariant operators except identity, and that is therefore simply isomorphic with its group of cogredient isomorphisms. In this section the groups for which this process leads to identity are classified according to the number of these successive groups of cogredient isomorphisms. Thus, abelian groups are of the first class; metabelian groups are of the second class; and groups that have metabelian groups of cogredient isomorphisms are of the third class.

Let G be a group of the third class. If the order of G is $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, where $p_1, p_2, \cdots, p_n$ are distinct primes, G is the direct product of groups of orders $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_n^{\alpha_n}$ respectively (see introduction). The class of each of these factor groups is not greater than 3. Every subgroup (and likewise every quotient group) of G is of the first, second, or third class. If a group is the direct product of factor groups whose orders are powers of distinct primes, and if the order of the group is not divisible by the fourth power of a prime, every one of these factor groups is of the first or second class, and the group itself is of the first or second class. Hence the order of every group of the third class is divisible by the fourth power of a prime.

Since a metabelian group is characterized by the property that all of its commutators are invariant (see introduction), it follows that a group of the third class is characterized by the property that those of its commutators formed by any of its commutators and any operator of the group are invariant.

If G is a group of the nth class and if A is an operator of G that corresponds to an invariant operator of G', then $A^{-1}CA = Ch$, C being any operator of G, and h an invariant commutator of G. If α is the order of the operator of G' that corresponds to A, then $A^{-\alpha}CA^{\alpha} = Ch^{\alpha} = C$. If now C runs through all the operators of G, h will run through a set of invariant commutators of G and α will be the order of some one of these. Hence the

order of every invariant operator of G' is the order of some invariant commutator of G.

If t is any non-invariant commutator of a group G of the third class, and if $B^{-1}CB = Ct$, $B^{-1}tB = th$, then $B^{-\beta}CB^{\beta} = Ct^{\beta}h^{\frac{1}{2}\beta(\beta-1)}$. If β is the order of the operator of G' that corresponds to B, then $t^{\beta}h^{\frac{1}{2}\beta(\beta-1)} = 1$, and if the order of G (and hence β), is odd, then $t^{\beta} = 1$. We have therefore proved the following:

THEOREM I.—*If G is a group of the third class, of odd order, the order of every commutator of G is the order of some operator of G'.*

If the order of G is even, the order of any commutator is at most twice the order of some operator of G'.

Let G be a group of the third class, of odd order, and let A_i $(i = 1, 2, \cdots, n)$ be operators of G that correspond respectively to the generators A_i' of G'. Also let $A_1^{-1}A_jA_1 = A_jt_j$, $A_1^{-1}t_jA_1 = t_jh_j$, and let β_j be the order of t_j. Then $A_1^{-\beta_j}A_jA_1^{\beta_j} = A_j$. Therefore if μ is the least common multiple of the β_j $(j = 2, 3, \cdots, n)$, A_1^{μ} is commutative with every operator of G; moreover, $A_1^{\mu'}$, where $\mu' < \mu$, is not commutative with every operator of G. We have therefore

THEOREM II.—*If G is a group of the third class, of odd order, the order of every operator of G' is the order of a commutator of G.*

In proving this theorem we assumed that in a group of the third class, of odd order, the least common multiple of the orders of any commutators is the order of a commutator. This is evidently the case in any group whose order is a power of a prime. Suppose now that G is a group of the third class of order $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, where $p_1, p_2, \cdots, p_n$ are distinct odd primes. It is the direct product of groups $G_1, G_2, \cdots, G_n$ of orders $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_n^{\alpha_n}$ respectively, and G' is the direct product of $G_1', G_2', \cdots, G_n'$.*

If G' has an operator of order $p_1^{\alpha_1'}p_2^{\alpha_2'}\cdots p_n^{\alpha_n'}$, then G_i' has an operator of order $p_i^{\alpha_i'}$ $(i = 1, 2, \cdots, n)$. Therefore G_i contains a commutator of order $p_i^{\alpha_i'}$. If we take such a commutator from each of the n factors groups and form their product, we shall get a commutator of G of order $p_1^{\alpha_1'}p_2^{\alpha_2'}\cdots p_n^{\alpha_n'}$.

If the order of G is even, the order of any operator of G' is either the order of some commutator of G, or twice the order of some commutator of G.

In general, if G is of the nth class, the least common multiple of the orders of any of its operators is the order of some operator.†

THEOREM III.—*A metabelian group G', of odd order, having a set of generators such that the order of one of them is not a divisor of the least common multiple of the orders of all the others, cannot be a group of cogredient isomorphisms.*

* MILLER, Bulletin of the American Mathematical Society, vol. 5 (1899), p. 294.

† The proof of this is similar to that given by FROBENIUS and STICKELBERGER, Crelle's Journal, vol. 86 (1879), p. 234, for operators of an abelian group.

Let A_i $(i = 1, 2, \cdots, n)$ be operators of G that correspond respectively to the generators A_i' of G'. Let α_i be the order of A_i'. Then

$$A_1^{-\alpha_i} A_i A_1^{\alpha_i} = A_i \qquad (i = 2, 3, \cdots, n).$$

If μ is the least common multiple of $\alpha_2, \alpha_3, \cdots, \alpha_n$, we have

$$A_1^{-\mu} A_i A_1^{\mu} = A_i.$$

Therefore A_1^{μ} is invariant in G, and α_i is a divisor of μ.

COROLLARY.—*If G' is of order p^α, where p is an odd prime, it must have at least two generators of the highest order.*

That the theorem does not hold for groups of even order is seen in the groups of order 16 of the third class. The group of cogredient isomorphisms of such a group is the non-quaternion group of order 8. This group is generated by an operator of order 4 and one of order 2. The more general statement of the theorem is as follows:

A metabelian group G' having a set of generators such that the order of any one of them is not a divisor of twice the least common multiple of the orders of all the others cannot be a group of cogredient isomorphisms.

If a group G' has a set of generators such that some operator A' (other than identity) of G' is a power of every one of these generators, G' cannot be a group of cogredient isomorphisms. For, if it could, the operators of G that correspond to A' would be invariant in G. In particular, no Hamiltonian group can be a group of cogredient isomorphisms.*

Hence if G is of the third class, of odd order, and has a cyclic commutator subgroup, G' must have invariant operators besides its commutators. For if it had no invariant operators besides its commutators, one of these commutators would be a power of every generator of G'. It follows from this that a group of order p^4 cannot have a cyclic commutator subgroup of order p^2 if p is an odd prime.

THEOREM IV.—*If the commutator subgroup of a group G of order p^α is of order p^β, where p is a prime, the class of G is equal to, or less than, $\beta + 1$.*

For if G is non-abelian and all its commutators are invariant, it is of the second class. If only $1/p$ of the operators of the commutator subgroup are invariant, G is of the third class. Therefore, if the commutator subgroup of G is of order p^2, G belongs to the second or third class. If now G' belongs to the class j, where $j \leqq i$, its commutator subgroup being of order p^{i-1}, it follows that the class of any group having G' for its group of cogredient isomorphisms is equal to, or less than, $i + 1$, and that the order of its commutator

* MILLER, Bulletin of the American Mathematical Society, vol. 6 (1900), p. 339.

subgroup is equal to, or greater than, p^i. It has just been shown that this supposition holds when $i = 3$. Therefore it holds for all values of i.

THEOREM V.—*If G is a group of the third class of order p^n, where p is a prime, and G' has a cyclic commutator subgroup, then the group of cogredient isomorphisms G'' of G' has just two independent generators.**

Since G' is metabelian and has a cyclic commutator subgroup, G'' must have an even number of independent generators. We shall show that there cannot be four of these generators and an obvious extension of the same argument will show that there cannot be any even number of them greater than two.

Let the four independent generators of G'' be A'', B'', C'', D''; and let A', B', C', D' be operators of G' that correspond respectively to these, while operators of G that correspond to A', B', C', D' are represented by A, B, C, D respectively. Let h_i $(i = 1, 2, \cdots)$ represent the invariant operators of G, t a commutator of G that corresponds to a generator of the cyclic commutator subgroup of G', and k_j $(j = 1, 2, \cdots)$ operators of G that correspond to the invariant operators of G' that are not commutators (if there be such operators). Let p^m be the order of the commutator subgroup of G'. Two of the independent generators of G'', say C'' and D'', will then be of order p^m, and the other two, A'' and B'', will be of order $p^{m-\beta}$, where $0 \leqq \beta < m$. Now, the commutator of G' formed by A' and B' is of order $p^{m-\beta}$, and that formed by C' and D' is of order p^m. Every operator of G' that corresponds to the subgroup of G'' generated by C'' and D'' is commutative with A' and B'; likewise every operator of G' that corresponds to the subgroup of G'' generated by A'' and B'' is commutative with C' and D'. Therefore

$$D^{-1}BD = Bh_1, \qquad D^{-1}CD = Cth_2, \qquad C^{-1}BC = Bh_3.$$

Hence

$$(Cth_2)^{-1}Bh_1(Cth_2) = Bh_1h_3,$$

and t is commutative with B. It can be shown in a similar way that t is commutative with k_j and A; also that t^{p^β} is commutative with C, and D. Therefore t^{p^β} is invariant in G. But this cannot be the case since $\beta < m$. The supposition that G'' has four independent generators leads therefore to a contradiction.

THEOREM VI.—*In any group G the operators that correspond to the invariant operators of G' are commutative with all the commutators of G.*

Let t be any commutator of G and let A_1 and A_2 be so chosen that

$$A_2^{-1}A_1A_2 = A_1t.$$

If k is any operator of G that corresponds to an invariant operator of G', then

* For a special case of this theorem, see YOUNG, *loc. cit.*, p. 178.

$$k^{-1}A_1k = A_1h_1, \qquad k^{-1}A_2k = A_2h_2,$$

where h_1 and h_2 are invariant operators of G.

Therefore

$$(kh_2^{-1})^{-1}A_1t(kh_2^{-1}) = A_1th_1,$$

and k is commutative with t.

We shall now prove that *there is one, and only one, group G of order p^5, where p is an odd prime, that has a cyclic commutator subgroup of order p^2.*

Such a group could not be abelian or metabelian. It must therefore be of the third class. Also G' must be of order p^4 of the type $(1,1)(1,1)$. It cannot have one generator of order greater than the orders of all the others, and it must contain an operator of order p^2, since G contains a commutator of order p^2. There is only one metabelian group of order p^4 that satisfies these conditions.* It is generated by the operators A' and B', where

$$A'^{p^2} = 1, \qquad B'^{p^2} = 1, \qquad B'^{-1}A'B' = A'^{1+p}.$$

Let t be a commutator of G of order p^2, and let A and B be operators of G that correspond respectively to A' and B' of G'. We may assume that A' has been so chosen that

$$A^p = t, \qquad B^{p^2} = t^{bp}, \qquad B^{-1}AB = A^{1+ap}, \qquad a \not\equiv 0 \pmod{p}.$$

If $b = 0$, these relations define a group. If $0 < b < p$, let $B_1 \equiv BA^{-b}$. Then $B_1^{p^2} = (BA^{-b})^{p^2} = B^{p^2}A^{-bp^2} = 1$. The group $\{A, B\}$ is identical with the group $\{A, B_1\}$. This is the same as the one obtained when $b = 0$.

This group is not found in the published list of groups of order p^5.† This list contains two groups of order 3^5 and one of order p^5 $(p > 3)$, whose commutator subgroups are cyclic of order p^2. It follows from Theorem III that these three groups do not exist.

Suppose that G is a group of order p^6 that has a cyclic commutator subgroup of order p^3, p being an odd prime. Such a group must be of the fourth class and its group of cogredient isomorphisms must be of order p^5 and must have a cyclic commutator subgroup of order p^2. We have just seen that there is only one such group. But it cannot be a group of cogredient isomorphisms since it is generated by an operator of order p^3 and one of order p^2. Hence, *there is no group of order p^6 that has a cyclic commutator subgroup of order p^3, p being an odd prime.*

* YOUNG, *loc. cit.*, p. 147; HÖLDER, Mathematische Annalen, vol. 43 (1893), pp. 409, 410.

† BAGNERA, Annali di Matematica, series III, vol. 1 (1898), pp. 137–228. It is given by BURNSIDE, *Theory of Groups of Finite Order*, 1897, p. 79.

If G is a group of the fourth class whose order is not divisible by 2 or 3, and if A_1 and A_2 are any two operators of G then

$$A_2^{-1} A_1 A_2 = A_1 t_1,$$

and

$$A_2^{-\alpha_1} A_1 A_2^{\alpha_1} = A_1 t_1^{\alpha_1} t_2^{\frac{\alpha_1(\alpha_1-1)}{2}} h_1^{\frac{\alpha_1(\alpha_1-1)(\alpha_1-2)}{2\cdot 3}} h_2^{\frac{\alpha_1(\alpha_1-1)(\alpha_1-2)}{2\cdot 3}},$$

where

$$A_2^{-1} t_1 A_2 = t_1 t_2, \qquad A_2^{-1} t_2 A_2 = t_2 h_1, \qquad t_1^{-1} t_2 t_1 = t_2 h_2,$$

h_1 and h_2 being invariant operators of G.

If G is of the fifth class, we have

$$A_2^{-\alpha_1} A_1 A_2^{\alpha_1} = A_1 t_1^{\alpha_1} t_2^{\frac{\alpha_1(\alpha_1-1)}{2}} t_3^{\frac{\alpha_1(\alpha_1-1)(\alpha_1-2)}{2\cdot 3}} h_1^{\frac{\alpha_1(\alpha_1-1)(\alpha_1-2)}{2\cdot 3}} h_2^{\frac{\alpha_1(\alpha_1-1)(\alpha_1-2)(\alpha_1-3)}{2\cdot 3\cdot 4}},$$

where

$$A_2^{-1} t_2 A_2 = t_2 t_3, \qquad t_1^{-1} t_2 t_1 = t_2 h_1, \qquad A_2^{-1} t_3 A_2 = t_3 h_2.$$

Now, if α_1 is the order of the operator of G' that corresponds to A_1, then the orders of t_1, t_2, t_3, h_1, h_2 are all divisors of α_1. Hence *in a group G of the fourth or fifth class whose order is not divisible by* 2 *or* 3, *an operator A_1 that corresponds to an operator of G' of order α_1 is commutative with the α_1 power of every operator of G.*

From this follows

THEOREM VII.—*A group G' of the third or fourth class whose order is not divisible by* 2 *or* 3 *cannot be a group of cogredient isomorphisms if it has a set of generators such that the order of one of them is not a divisor of the least common multiple of the orders of all the others.*

CORNELL UNIVERSITY, *June*, 1901.

CONJUGATE RECTILINEAR CONGRUENCES*

BY

LUTHER PFAHLER EISENHART

Introduction.

CIFARELLI† has established certain formulæ showing the relation existing between the Kummer functions of a rectilinear congruence referred to a general double family of parametric ruled surfaces of the congruence. In § 1 we have applied these formulæ to several special cases—afforded by taking in turn for the double family of parametric ruled surfaces the principal surfaces, the mean ruled surfaces, and one family of the developables and their orthogonal trajectories—for the determination of all congruences having a given spherical representation of any one of these three double families. In each case we find that the abscissa, measured from the surface of reference, of the point where the line of shortest distance between the lines $(u, v), (u + du, v)$ meets the former line satisfies a partial differential equation of the second order whose coefficients involve the coefficients of the fundamental quadratic differential form of the sphere. When this abscissa has been found, the further determination reduces to the solution of a Riccati equation and quadratures.

In § 2 we restrict ourselves to systems upon the sphere consisting of a family of great circles, $u = \text{const.}$, and their orthogonal trajectories, $v = \text{const.}$ Having shown that the line of shortest distance between the lines $(u, v), (u + du, v)$ has a different direction from the line of shortest distance between the latter and the consecutive line in the ruled surface $v = \text{const.}$ which passes through the line (u, v), we consider the congruence of lines upon which the shortest distances are measured and call it a *conjugate* of the original congruence. Evidently for each choice of a family of great circles on the sphere there is a conjugate of a given congruence, hence the conjugate is not determinate until the parametric system of curves is given. The above definition fails when the ruled surfaces $v = \text{const.}$ are developables, but another definition, consistent with the former, removes this exception.

In § 3, certain relations are found to hold between the Kummer functions of a congruence and any of its conjugates, from which one finds the equation of

* Presented to the Society October 26, 1901. Received for publication Nov. 5, 1901.

† *Le Congruence*, Annali di Matematica, ser. 3, vol. 2 (1899), p. 139.

condition that a conjugate congruence of a normal congruence be normal. In order that the lines of a conjugate congruence of a normal congruence be tangent to one of the orthogonal surfaces of the latter, they must be tangents to asymptotic lines upon this surface.

It is shown in § 5 that when a family of great circles and their orthogonal trajectories are given, the determination of the direction cosines is the same problem as the finding of a skew curve from its intrinsic equations.

In §§ 6, 7 three cases are discussed, according as a given system of great circles and their orthogonal trajectories are the spherical representation of the principal ruled surfaces, of the mean ruled surfaces, or of one family of developables and the ruled surfaces of the congruence cutting them orthogonally. In particular, those congruences are considered for which the corresponding conjugate congruences have ruled surfaces of like character in correspondence. Of special interest is the result that, when a congruence and the conjugate which corresponds to its developables are normal congruences, the developables correspond and the determination of all such congruences with a given spherical representation of their developables reduces to quadratures.

§ 1. *Determination of congruences with a given spherical representation of particular ruled surfaces.*

Consider a rectilinear congruence referred to a general system of parameters, u, v. Let X, Y, Z denote the direction cosines of any line Γ of the congruence, and x, y, z, the cartesian coördinates of the point where the line meets the surface of reference. Write

$$(1)\qquad E=\sum\left(\frac{\partial X}{\partial u}\right)^2,\quad F=\sum\frac{\partial X}{\partial u}\frac{\partial X}{\partial v},\quad G=\sum\left(\frac{\partial X}{\partial v}\right)^2,$$

$$e=\sum\frac{\partial x}{\partial u}\frac{\partial X}{\partial u},\quad f=\sum\frac{\partial x}{\partial v}\frac{\partial X}{\partial u},\quad f'=\sum\frac{\partial x}{\partial u}\frac{\partial X}{\partial v},\quad g=\sum\frac{\partial x}{\partial v}\frac{\partial X}{\partial v}.$$

These are the KUMMER functions, and CIFARELLI* has shown that they are connected by the following relations:

$$(2)\qquad \begin{aligned}\frac{\partial x}{\partial u}&=\frac{eG-f'F}{EG-F^2}\frac{\partial X}{\partial u}+\frac{f'E-eF}{EG-F^2}\frac{\partial X}{\partial v}+AX,\\ \frac{\partial x}{\partial v}&=\frac{fG-gF}{EG-F^2}\frac{\partial X}{\partial u}+\frac{gE-fF}{EG-F^2}\frac{\partial X}{\partial v}+BX,\end{aligned}$$

where

$$(3)\qquad A=\sum X\frac{\partial x}{\partial u},\quad B=\sum X\frac{\partial X}{\partial v}.$$

* l. c., p. 141.

The expressions in y and z follow at once by analogy. The condition of integrability of (2) leads to the following relations:

$$\begin{aligned}
&\frac{\partial e}{\partial v} - \frac{\partial f}{\partial u} - \begin{Bmatrix} 12 \\ 1 \end{Bmatrix}' e + \begin{Bmatrix} 11 \\ 1 \end{Bmatrix}' f - \begin{Bmatrix} 12 \\ 2 \end{Bmatrix}' f' \\
&\qquad\qquad + \begin{Bmatrix} 11 \\ 2 \end{Bmatrix}' g + FA - EB = 0, \\
&\frac{\partial f'}{\partial v} - \frac{\partial g}{\partial u} - \begin{Bmatrix} 22 \\ 1 \end{Bmatrix}' e + \begin{Bmatrix} 12 \\ 1 \end{Bmatrix}' f - \begin{Bmatrix} 22 \\ 2 \end{Bmatrix}' f' \\
&\qquad\qquad + \begin{Bmatrix} 12 \\ 2 \end{Bmatrix}' g + GA - FB = 0, \\
&\frac{\partial A}{\partial v} - \frac{\partial B}{\partial u} + f - f' = 0,
\end{aligned} \tag{4}$$

where the Christoffel symbols $\left\{ \begin{smallmatrix} rs \\ t \end{smallmatrix} \right\}'$ are formed with respect to the quadratic form

$$E du^2 + 2F du\, dv + G dv^2. \tag{5}$$

We now apply these general results to several particular cases.

Consider first the case where the spherical representation is that of the *principal* ruled surfaces of the congruence, and take for the surface of reference the middle surface of the congruence. From this hypothesis we have *

$$F = 0, \qquad f + f' = 0, \qquad eG + gE = 0. \tag{6}$$

Indicating by r the abscissa of the limit point corresponding to the lines (u, v), $(u + du, v)$, we have in consequence of the last equation of (6) †

$$r = -\frac{e}{E} = \frac{g}{G}. \tag{7}$$

In conformity with the second equation of (6) we introduce with BIANCHI ‡ a new function ϕ defined by

$$f = \phi \sqrt{EG}, \qquad f' = -\phi \sqrt{EG}. \tag{8}$$

Substituting these expressions for e, f, f', g, F in (2) and replacing A and B by their values given in the first two of equations (4), we have for the mean surface

* BIANCHI, *Lezioni*, p. 258.

† l. c., p. 247.

‡ l. c., p. 275.

$$
\begin{aligned}
\frac{\partial x}{\partial u} &= -r\frac{\partial X}{\partial u} - \sqrt{\frac{E}{G}}\phi\frac{\partial X}{\partial v} + \left(\sqrt{\frac{E}{G}}\frac{\partial \phi}{\partial v} + \frac{1}{G}\frac{\partial (rG)}{\partial u}\right)X, \\
\frac{\partial x}{\partial v} &= r\frac{\partial X}{\partial v} + \sqrt{\frac{G}{E}}\phi\frac{\partial X}{\partial u} - \left(\frac{1}{E}\frac{\partial (rE)}{\partial v} + \sqrt{\frac{G}{E}}\frac{\partial \phi}{\partial u}\right)X,
\end{aligned} \tag{9}
$$

with analogous expressions in y and z. And the third of equations (4) reduces to

$$
\begin{aligned}
2\frac{\partial^2 r}{\partial u\,\partial v} + \frac{\partial \log E}{\partial v}\frac{\partial r}{\partial u} + \frac{\partial \log G}{\partial u}\frac{\partial r}{\partial v} + \frac{\partial^2 \log EG}{\partial u\,\partial v}r \\
= -\left[\frac{\partial}{\partial u}\left(\sqrt{\frac{G}{E}}\frac{\partial \phi}{\partial v}\right) + \frac{\partial}{\partial v}\left(\sqrt{\frac{E}{G}}\frac{\partial \phi}{\partial u}\right)\right] - 2\sqrt{EG}\,\phi,
\end{aligned} \tag{10}
$$

which is the necessary and sufficient condition which r and ϕ must satisfy in order that the congruence shall have the given representation of its principal surfaces. Evidently one of these functions can be chosen arbitrarily and the other is determined by the integration of an equation of Laplace.

In the second case we consider the determination of congruences with a given spherical representation of their *mean ruled surfaces*. As defined by CIFARELLI,* the mean ruled surfaces form a double system, in general unique, for which the surfaces of one family cut those of the other family orthogonally, and the lines of striction of the two surfaces which pass through any line meet the latter in its middle point. When the congruence is referred to a general parametric system, the directions of the spherical representation of the mean ruled surfaces are given by the equation obtained by equating to zero the Jacobian of equation (5) and of the left-hand member of the general equation for the directions of the principal ruled surfaces.† This gives

$$
\begin{aligned}
&\{E(gE-eG) - F[(f+f')E - 2eF]\}du^2 \\
&\quad + 2[F(gE+eG) - (f+f')EG]\,du\,dv \\
&\quad + \{F[2gF - (f+f')G] - G(gE-eG)\}dv^2 = 0.
\end{aligned} \tag{11}
$$

In order that the parametric curves on the sphere be the images of the mean surfaces, it is necessary and sufficient that

$$
gE - eG = 0, \qquad F = 0; \tag{12}
$$

and if we take one of the limit surfaces for the surface of reference, we must have‡

---

*Annali di Matematica, ser. 3, vol. 2 (1899), p. 151.

† BIANCHI, *Lezioni*, p. 251.

‡ l. c., p. 251.

$$eg - \left(\frac{f+f'}{2}\right)^2 = 0, \tag{13}$$

and conversely. From (12) we get

$$r = -\frac{e}{E} = -\frac{g}{G}; \tag{14}$$

and in conformity with (13) we introduce a new function ϕ, defined by

$$\frac{f}{\sqrt{EG}} = -r + \phi, \qquad \frac{f'}{\sqrt{EG}} = -(r + \phi). \tag{15}$$

Proceeding as in the former case we obtain

$$\begin{aligned} \frac{\partial x}{\partial u} &= -r\frac{\partial X}{\partial u} - \sqrt{\frac{E}{G}}(r+\phi)\frac{\partial X}{\partial v} \\ &\quad -\left(\frac{\partial r}{\partial u} - \sqrt{\frac{E}{G}}\frac{\partial}{\partial v}(r+\phi) - \frac{1}{\sqrt{EG}}\frac{\partial E}{\partial v}r\right)X, \\ \frac{\partial x}{\partial v} &= -\sqrt{\frac{G}{E}}(r-\phi)\frac{\partial X}{\partial u} - r\frac{\partial X}{\partial v} \\ &\quad -\left(\frac{\partial r}{\partial v} - \sqrt{\frac{G}{E}}\frac{\partial}{\partial u}(r-\phi) - \frac{1}{\sqrt{EG}}\frac{\partial G}{\partial u}r\right)X, \end{aligned} \tag{16}$$

and similar equations in y and z. Again we find that the functions r and ϕ satisfy a condition of the second order; it is

$$\begin{aligned} &\sqrt{\frac{G}{E}}\frac{\partial^2 r}{\partial u^2} - \sqrt{\frac{E}{G}}\frac{\partial^2 r}{\partial v^2} + \left(\frac{\partial}{\partial u}\sqrt{\frac{G}{E}} + \frac{1}{\sqrt{EG}}\frac{\partial G}{\partial u}\right)\frac{\partial r}{\partial u} \\ &-\left(\frac{\partial}{\partial v}\sqrt{\frac{E}{G}} + \frac{1}{\sqrt{EG}}\frac{\partial E}{\partial v}\right)\frac{\partial r}{\partial v} + \left[\frac{\partial}{\partial u}\left(\frac{1}{\sqrt{EG}}\frac{\partial G}{\partial u}\right) - \frac{\partial}{\partial v}\left(\frac{1}{\sqrt{EG}}\frac{\partial E}{\partial v}\right)\right]r \\ &\qquad = \frac{\partial}{\partial u}\left(\sqrt{\frac{G}{E}}\frac{\partial \phi}{\partial u}\right) + \frac{\partial}{\partial v}\left(\sqrt{\frac{E}{G}}\frac{\partial \phi}{\partial v}\right) + 2\sqrt{EG}\phi. \end{aligned} \tag{17}$$

In the third case, we seek to determine the congruences for which one family of developables is represented by a given family of curves upon the sphere. Let $v = \text{const.}$ represent these curves and let $u = \text{const.}$ be their orthogonal trajectories; then $F = 0$. From the general equation for the direction of the developables * we find for this choice of parameters

$$f' = 0. \tag{18}$$

* l. c., p. 252.

Take for the surface of reference the locus of the points half way between the focal point given by the lines (u, v), $(u + du, v)$, and the point where the line of shortest distance between the lines (u, v), $(u, v + dv)$ meets the former line; then

$$r = -\frac{e}{E} = \frac{g}{G}. \tag{19}$$

If we put

$$\frac{f}{E} = \phi, \tag{20}$$

the surface of reference is given by

$$\begin{aligned} \frac{\partial x}{\partial u} &= -r\frac{\partial X}{\partial u} + \left(\frac{\partial r}{\partial u} + r\frac{\partial \log G}{\partial u} - \frac{1}{2G}\frac{\partial E}{\partial v}\phi\right)X, \\ \frac{\partial x}{\partial v} &= \phi\frac{\partial X}{\partial u} + r\frac{\partial X}{\partial v} - \left(\frac{\partial r}{\partial v} + r\frac{\partial \log E}{\partial v} + \frac{\partial \phi}{\partial u} + \frac{\partial \log \sqrt{E}}{\partial u}\phi\right)X, \end{aligned} \tag{21}$$

and similar equations in y and z. And the functions ϕ, r, satisfy the condition

$$\begin{aligned} 2\frac{\partial^2 r}{\partial u\,\partial v} + \frac{\partial \log E}{\partial v}\frac{\partial r}{\partial u} + \frac{\partial \log G}{\partial u}\frac{\partial r}{\partial v} + \frac{\partial^2 \log EG}{\partial u\,\partial v}r \\ = -\left[\frac{\partial^2 \phi}{\partial u^2} + \frac{\partial \log \sqrt{E}}{\partial u}\frac{\partial \phi}{\partial u} - \frac{1}{2G}\frac{\partial E}{\partial v}\frac{\partial \phi}{\partial v}\right. \\ \left. + \phi\left(\frac{1}{2G^2}\frac{\partial E}{\partial v}\frac{\partial G}{\partial v} - \frac{1}{2G}\frac{\partial^2 E}{\partial v^2} + \frac{\partial^2 \log \sqrt{E}}{\partial u^2} + E\right)\right]. \end{aligned} \tag{22}$$

In all three cases the congruence is normal when $\phi = 0$. Furthermore, when this condition is satisfied, the first and third cases are the same.

§ 2. *Definition of conjugate congruences.*

Let λ, μ, ν denote the direction-cosines of the line of shortest distance between the lines (u, v), $(u + du, v + dv)$ of a congruence referred to a general parametric system. It can be shown that *

$$\lambda = \frac{\left(E\frac{\partial X}{\partial v} - F\frac{\partial X}{\partial u}\right)du + \left(F\frac{\partial X}{\partial v} - G\frac{\partial X}{\partial u}\right)dv}{\sqrt{EG - F^2}\sqrt{Edu^2 + 2Fdu\,dv + Gdv^2}},$$

and similarly for μ and ν. If in particular we denote by X_1, Y_1, Z_1; X_2, Y_2, Z_2

* BIANCHI, l. c., p. 246.

the direction cosines of the line of shortest distance from the line (u, v) to $(u+du, v)$ and $(u, v+dv)$ respectively, we have from the preceding formula

$$X_1 = \frac{E\frac{\partial X}{\partial v} - F\frac{\partial X}{\partial u}}{\sqrt{E}\sqrt{EG-F^2}}, \qquad Y_1 = \frac{E\frac{\partial Y}{\partial v} - F\frac{\partial Y}{\partial u}}{\sqrt{E}\sqrt{EG-F^2}},$$

(23)

$$Z_1 = \frac{E\frac{\partial Z}{\partial v} - F\frac{\partial Z}{\partial u}}{\sqrt{E}\sqrt{EG-F^2}};$$

$$X_2 = \frac{F\frac{\partial X}{\partial v} - G\frac{\partial X}{\partial u}}{\sqrt{G}\sqrt{EG-F^2}}, \qquad Y_2 = \frac{F\frac{\partial Y}{\partial v} - G\frac{\partial Y}{\partial u}}{\sqrt{G}\sqrt{EG-F^2}},$$

(24)

$$Z_2 = \frac{F\frac{\partial Z}{\partial v} - G\frac{\partial Z}{\partial u}}{\sqrt{G}\sqrt{EG-F^2}}.$$

From these we find upon differentiation and reduction

$$\frac{\partial X_1}{\partial u} = -\frac{\sqrt{EG-F^2}}{E^2}\begin{Bmatrix}11\\2\end{Bmatrix}'\frac{\partial X}{\partial u},$$

(25)

$$\frac{\partial X_1}{\partial v} = -\frac{\sqrt{EG-F^2}}{E^2}\left(\begin{Bmatrix}12\\2\end{Bmatrix}'\frac{\partial X}{\partial u} + EX\right),$$

$$\frac{\partial X_2}{\partial u} = \frac{\sqrt{EG-F^2}}{G^2}\left(\begin{Bmatrix}12\\1\end{Bmatrix}'\frac{\partial X}{\partial v} + GX\right),$$

(26)

$$\frac{\partial X_2}{\partial v} = \frac{\sqrt{EG-F^2}}{G^2}\begin{Bmatrix}22\\1\end{Bmatrix}'X,$$

and similar equations in the Y's and Z's.

The necessary and sufficient condition that the elements of any ruled surface $u = \text{const.}$ of a congruence be parallel to a plane, whose direction varies with the value of this constant, is that the surface be represented on the sphere by a great circle. The analytical expression of this condition is*

$$\begin{Bmatrix}22\\1\end{Bmatrix}' = 0. \tag{27}$$

In this case, as is seen from (26), X_2, Y_2, Z_2 are functions of u alone, and conse-

* BIANCHI, l. c., p. 146.

quently all the lines of shortest length between consecutive lines of a ruled surface $u = \text{const.}$ have the same direction. Conversely, when this property is possessed by all of the surfaces $u = \text{const.}$, it is necessary that

$$\left\{ \begin{matrix} 22 \\ 1 \end{matrix} \right\}' \frac{\partial X}{\partial v} = \left\{ \begin{matrix} 22 \\ 1 \end{matrix} \right\}' \frac{\partial Y}{\partial v} = \left\{ \begin{matrix} 22 \\ 1 \end{matrix} \right\}' \frac{\partial Z}{\partial v} = 0.$$

Since one at least of the functions X, Y, Z must be a function of v, the above equations are satisfied only by the condition (27). Hence the

THEOREM.— *When all the lines of shortest length between consecutive lines of any surface in a family of ruled surfaces of a congruence have the same direction, the generatrices are parallel to a plane which is different for different surfaces of the family.*

We assume that the sphere is referred to a family of great circles and their orthogonal trajectories. Then (27) is satisfied, and by a proper choice of parameters we have *

$$F = 0, \qquad G = 1. \tag{28}$$

Consider in connection with the given congruence C the system of lines upon which is measured the shortest distances between the lines $(u, v), (u + du, v)$ of C. In order that this system of lines be a congruence C_1, it is sufficient that to each line Γ of C there corresponds a unique line Γ_1 of C_1. This would fail to occur only when the lines of shortest distance between three consecutive generatrices in a ruled surface $v = \text{const.}$ coincide, in which case the three generatrices would be parallel to the same plane. Hence from what has preceded we see that the sufficient condition that there be a unique line Γ_1 for each line Γ is given by

$$\frac{\partial X_1}{\partial u} \neq 0, \qquad \frac{\partial Y_1}{\partial u} \neq 0, \qquad \frac{\partial Z_1}{\partial u} \neq 0.$$

For from (25) it is clear that if these conditions were not satisfied we would have

$$\left\{ \begin{matrix} 11 \\ 2 \end{matrix} \right\}' = 0,$$

that is,† the lines $v = \text{const.}$ on the sphere would be great circles. Since there cannot exist upon a sphere an orthogonal system of great circles we are brought to the

THEOREM.— *When a family of great circles $u = \text{const.}$ and their orthogonal trajectories are the spherical representation of a congruence, the lines upon*

* BIANCHI, l. c., p. 154.

† l. c., p. 146.

which are measured the shortest distances between the lines (u, v), $(u + du, v)$ *from a congruence.*

We say that the latter congruence is *conjugate* to the former.

In consequence of the choice of parameters giving (28) the formulæ (23), (24) take the forms

$$X_1 = \frac{\partial X}{\partial v}, \qquad \frac{\partial X_1}{\partial u} = \frac{\partial \log \sqrt{E}}{\partial v}\frac{\partial X}{\partial u}, \qquad \frac{\partial X_1}{\partial v} = -X. \tag{29}$$

These forms lead to an extension of the definition to an exceptional case.

Since consecutive generatrices of a developable surface intersect, the line of shortest distance between them is indeterminate. Consequently, if the ruled surfaces $v = \text{const.}$ of the congruence C are developables, the conjugate C_1, as above defined, would have no meaning. In accordance with the first equation of (29) we define the corresponding congruence C_1 in this case as the double system of lines with direction cosines equal to $\partial X/\partial v$, $\partial Y/\partial v$, $\partial Z/\partial v$ which pass through the corresponding focal points of the lines Γ.

Denote by E_1, F_1, G_1 the coefficients of the spherical representation of C_1; then from (29) we have

$$E_1 = \left(\frac{\partial \sqrt{E}}{\partial v}\right)^2, \qquad F_1 = 0, \qquad G_1 = 1. \tag{30}$$

From this it follows that the curves $u = \text{const.}$ on the sphere for C_1 are great circles, and consequently the generatrices of any one of the ruled surfaces $u = \text{const.}$ of C_1 are parallel to a plane. It follows from analogy that the direction-cosines of the conjugate of C_1 are $\partial X_1/\partial v$, $\partial Y_1/\partial v$, $\partial Z_1/\partial v$; but by (29) these are equal to $-X$, $-Y$, $-Z$; that is, the image of this line on the sphere is diametrically opposite the corresponding point for the original congruence. It can be seen geometrically that this line not only has the same direction as the corresponding line of C but actually coincides with it. Hence the

THEOREM.—*The conjugate of any conjugate of a congruence is this congruence itself with the positive direction of the lines reversed.*

§ 3. *Relations between a congruence and any conjugate.*

Let x_1, y_1, z_1 denote the cartesian coördinates of the point on the surface of reference S_1 of C_1 in which it is met by the line $\Gamma_1(u, v)$. If r and r_1 denote the distances from S and S_1 respectively of the point of intersection of Γ and Γ_1, we have

$$x + rX = x_1 + r_1 X_1, \qquad y + rY = y_1 + r_1 Y_1, \qquad z + rZ = z_1 + r_1 Z_1.$$

With the aid of (29) we find

$$(31)\qquad \begin{cases} \dfrac{\partial \log \sqrt{E}}{\partial v}(e+rE) = e_1 + r_1 E_1, \qquad f\dfrac{\partial \log \sqrt{E}}{\partial v} = f_1, \\ -\left(\sum X \dfrac{\partial x}{\partial u} + \dfrac{\partial r}{\partial u}\right) = f_1', \qquad -\left(\sum X \dfrac{\partial x}{\partial v} + \dfrac{\partial r}{\partial v}\right) = g_1 + r_1, \end{cases}$$

where the subscripts denote that the functions belong to C_1.

When C is a normal congruence, $f = f'$, and we find from (31) that the necessary and sufficient condition that C_1 also be normal is

$$(32)\qquad \sum X \frac{\partial x}{\partial u} + \frac{\partial r}{\partial u} + \frac{\partial \log \sqrt{E}}{\partial v} f' = 0.$$

The equation $f = f'$ is obtained from the condition that $\sum X dx$ shall be an exact differential, that is,

$$\sum X dx + d\rho = 0.$$

From this equation it follows also that ρ is the abscissa of the point where the line (u, v) of the congruence is met by one of the orthogonal surfaces. We take this surface for the surface of reference S; then $\rho = 0$ and

$$(33)\qquad e = -D, \qquad f = f' = -D', \qquad g = -D'',$$

where D, D', D'' are the coefficients of the second fundamental quadratic form of S. In order that the functions ρ and r may be the same and the tangents to the curves $v =$ const. on S form a congruence C_1, it is necessary and sufficient that $r = 0$, or, from (33),

$$D = 0;$$

that is, the curves $v =$ const. on S must be asymptotic. Hence the

THEOREM.—*The necessary and sufficient condition that the tangents to a family of curves on a surface form a conjugate to the congruence of normals is that the curves be asymptotic lines and be represented upon the sphere by the orthogonal trajectories of a family of great circles.*

It is evident that there is only a particular class of surfaces possessing this latter property. Since the normals to a ruled surface along a generatrix are parallel to a plane it follows that for ruled surfaces of this class the non-linear asymptotic lines are the ones referred to. For future purposes we will determine all minimal surfaces of this category.

It is well known that minimal surfaces are characterized by the property that their asymptotic lines are orthogonal, and that when these lines are taken as parametric the square of the linear element of the surface and spherical representation are * respectively

* BIANCHI, l. c., p. 126.

$$ds^2 = \rho(du^2 + dv^2), \qquad ds'^2 = \frac{1}{\rho}(du^2 + dv^2),$$

where $-1/\rho^2$ is equal to the total curvature of the surface. If the curves $u = \text{const.}$ on the sphere are to be great circles, ρ must be a function of v alone, and consequently the asymptotic lines $u = \text{const.}$ on the surface are geodesics, that is, straight lines. As the helicoid with plane director is the only ruled minimal surface, we have the

THEOREM.—*The only minimal surface for which one family of asymptotic lines is represented by a family of geodesic parallels on the sphere is the helicoid with plane director.*

We return now to the consideration of the congruences of normals to any of the particular class of surfaces referred to above. From (31) we have

$$r_1 = -g_1.$$

Hence the ruled surfaces $u = \text{const.}$, $v = \text{const.}$ of C, are such that

$$\frac{e_1}{E_1} = \frac{g_1}{G_1}, \qquad F = 0,$$

and therefore by (14) they are the mean ruled surfaces of C_1. Hence *the point of tangency of any tangent to the curves $v = \text{const.}$ is the mean point.* Were this point to be the mean point of Γ also, the surface S would be minimal. These results may be stated as follows:

The tangents to the helices on a helicoid with plane director form a congruence conjugate to the congruence of normals, and the helicoid is the mean surface for each congruence. Moreover, this is the only normal congruence possessing this double property.

Since the lines $v = \text{const.}$ on any of these surfaces are curved asymptotic lines and consequently not geodesics, we have the

THEOREM.—*When C is a normal congruence and C_1 is composed of the tangents to the asymptotic lines on one of the orthogonal surfaces, C_1 is not a normal congruence.*

§ 4. *Determination of a conjugate congruence when the original congruence is defined in a particular way.*

A congruence for which all the generatrices of any ruled surface $u = \text{const.}$ are parallel to a plane may be defined by equations of the form

$$(33') \qquad lx + my + nz = f_1(u, v), \qquad \lambda x + \mu y + \nu z = f_2(u, v),$$

where l, m, n are functions of u alone and λ, μ, ν are functions of u and v. If X, Y, Z denote the direction cosines, we have

$$lX + mY + nZ = 0.$$

By differentiation with respect to v, we have in view of (29),

$$lX_1 + mY_1 + nZ_1 = 0.$$

Hence the ruled surfaces $u = c$ of C and $u = c$ of C_1 have their generatrices parallel to the same plane. From this it follows that the great circles $u = \text{const.}$ for C_1 are the same as for C, and from the definition of conjugate congruences it follows that corresponding points are at the distance of a quadrant.

Denote by Γ and Γ' the lines (u, v), $(u + du, v)$ of C and by Γ_1 their line of shortest distance. From (33′) we have

$$X,\ Y,\ Z = \frac{m\nu - \mu n,\ n\lambda - \nu l,\ l\mu - m\lambda}{[\Sigma(m\nu - \mu n)^2]^{\frac{1}{2}}},$$

and if X', Y', Z' denote the direction-cosines of Γ', they are given by

$$X',\ Y',\ Z' = X + \frac{\partial X}{\partial u}du,\quad Y + \frac{\partial Y}{\partial u}du,\quad Z + \frac{\partial Z}{\partial u}du.$$

Hence, when (33′) is given, the functions $X, \cdots, Z'$ can be calculated at once. The equation of the plane determined by Γ' and Γ_1 is

$$(34)\qquad \begin{vmatrix} x - x_1 & y - y_1 & z - z_1 \\ X' & Y' & Z' \\ YZ' - ZY' & ZX' - XZ' & XY' - YX' \end{vmatrix} = 0,$$

where x, y, z are current coördinates and x_1, y_1, z_1 are the coördinates of the intersection of Γ' and Γ_1. These coördinates are given by the equations

$$(35)\qquad \begin{cases} lx_1 + my_1 + nz_1 = f_1(u, v), \\ \dfrac{\partial l}{\partial u}x_1 + \dfrac{\partial m}{\partial u}y_1 + \dfrac{\partial n}{\partial u}z_1 = \dfrac{\partial f_1}{\partial u}, \\ \left(\lambda + \dfrac{\partial \lambda}{\partial u}du\right)x_1 + \left(\mu + \dfrac{\partial \mu}{\partial u}du\right)y_1 + \left(\nu + \dfrac{\partial \nu}{\partial u}du\right)z_1 = 0. \end{cases}$$

Since the plane (34) passes through the intersection of Γ and Γ_1, we see that if the expressions for x_1, y_1, z_1 obtained from (35) are put in (34) and this equation is combined with (33′), we can find the coördinates of the point where Γ meets Γ_1.

From the definition of C_1 and the results found above, we find that C_1 is given by the equations

$$(33'')\qquad lx + my + nz = f_1(u, v),\qquad \lambda_1 x + \mu_1 y + \nu_1 z = f_3(u, v),$$

where λ_1, μ_1, ν_1 are functions of u and v satisfying the condition

$$\Sigma(m\nu - \mu n)(m\nu_1 - \mu_1 n) = 0,$$

and where $f_3(u, v)$ is determined by the condition that the plane defined by the second of equations (33″) passes through the intersection of Γ and Γ_1. Hence:

When a congruence is defined in the form (33′) *the corresponding conjugate congruence can be found without integration.*

§ 5. *Determination of the direction cosines when the system on the sphere is given.*

Consider the sphere referred to a parametric system such that

$$F = 0, \qquad G = 1. \tag{28}$$

The Gauss equation * reduces to

$$\frac{\partial^2 \sqrt{E}}{\partial v^2} + \sqrt{E} = 0,$$

whence

$$\sqrt{E} = U_1 \cos v + U_2 \sin v, \tag{36}$$

where U_1, U_2 are functions of u alone.

Denoting by λ_1, μ_1, ν_1; λ_2, μ_2, ν_2 the direction cosines of the tangents to the curves $v =$ const. and $u =$ const. respectively on the sphere, we have †

$$d\lambda_2 = \frac{\partial \sqrt{E}}{\partial v}\lambda_1 du - X dv, \qquad dX = \sqrt{E}\,\lambda_1 du + \lambda_2 dv, \tag{37}$$

and similar relations between Y, μ_1, μ_2 and Z, ν_1, ν_2. From these equations we find that

$$\frac{\partial^2 X}{\partial v^2} + X = 0,$$

from which it follows that

$$X = U_{11} \cos v + U_{12} \sin v, \tag{37′}$$

where U_{11}, U_{12} are functions of u alone; similarly for Y, Z. The functions of u appearing in these expressions must satisfy the following conditions:

$$U_{11}^2 + U_{21}^2 + U_{31}^2 = 1, \quad U_{12}^2 + U_{22}^2 + U_{32}^2 = 1, \quad U_{11}U_{12} + U_{21}U_{22} + U_{31}U_{32} = 0. \tag{38}$$

Again from equations (37) we find

---

*Bianchi, l. c., p. 67.

† l. c., p. 94.

$$\frac{\partial \lambda_2}{\partial u} = \frac{\partial \log \sqrt{E}}{\partial v} \frac{\partial X}{\partial u},$$

from which it follows that

$$U_1 U'_{11} - U_2 U'_{12} = 0,$$

where the accents denote differentiation; similarly for the functions $U_{21}, \cdots, U_{32}$.

Substituting the above expressions for E, X, Y, Z in

$$E = \sum \left(\frac{\partial X}{\partial u} \right)^2,$$

we find the following relations:

$$\sum U'^2_{11} = U_1^2, \qquad \sum U'^2_{12} = U_2^2, \qquad \sum U'_{11} U'_{12} = U_1 U_2.$$

By means of the preceding systems of equations we find readily the following relations:

$$(39) \quad \begin{aligned} \frac{U'_{11}}{U_{21}U_{32} - U_{31}U_{22}} &= \frac{U'_{21}}{U_{31}U_{12} - U_{11}U_{32}} = \frac{U'_{31}}{U_{11}U_{22} - U_{21}U_{12}} = U_1, \\ \frac{U'_{12}}{U_{21}U_{32} - U_{31}U_{22}} &= \frac{U'_{22}}{U_{31}U_{12} - U_{11}U_{32}} = \frac{U'_{32}}{U_{11}U_{22} - U_{21}U_{12}} = U_2. \end{aligned}$$

The equations of condition (38), (39) are those which would obtain if

$$U_{11}, \quad U_{21}, \quad U_{31}; \quad U_{12}, \quad U_{22}, \quad U_{32}$$

were the direction cosines of the tangent and binormal respectively of a curve with curvature U_1 and torsion U_2. Hence we have the following

THEOREM.—*The problem of finding the direction cosines of the lines of a congruence for which the parametric ruled surfaces in one family are represented by great circles is equivalent to the complete determination of a skew curve from its intrinsic equations.*

As is well known, the latter requires the solution of a Riccati equation.

Conversely, when the direction cosines of the lines of a congruence can be expressed in the form (37′) where $U_{11}, \cdots, U_{32}$ satisfy conditions (38) and

$$\frac{U'_{11}}{U'_{12}} = \frac{U'_{21}}{U'_{22}} = \frac{U'_{31}}{U'_{32}},$$

the ruled surfaces $u = \text{const.}$ have a family of great circles for their spherical representation.

§ 6. *When the system on the sphere is the image of the principal surfaces.*

Let the great circles $u = \text{const.}$ on the sphere be the spherical representation of one family of principal ruled surfaces. The equation (10) reduces to the form:

$$\frac{\partial}{\partial u}\left(2\frac{\partial r}{\partial v}+\frac{\partial \log E}{\partial v}r\right)$$

$$(40)\qquad =-\left[\frac{\partial}{\partial u}\left(\frac{1}{\sqrt{E}}\frac{\partial \phi}{\partial v}\right)+\frac{\partial}{\partial v}\left(\sqrt{E}\frac{\partial \phi}{\partial u}\right)+2\phi\sqrt{E}\right].$$

When ϕ is given an arbitrary form, r is obtained by quadratures. Hence the

THEOREM.—*The determination of all congruences for which one family of the principal ruled surfaces is represented on the sphere by a family of great circles reduces to quadratures, after the direction cosines of the lines of the congruence have been found.*

With every congruence C, whose principal ruled surfaces have a given spherical representation, there is associated a unique conjugate congruence C_1, determined by this parametric system. From (31) we find that the necessary and sufficient condition that the principal surfaces of C_1 correspond to those of C is given by the equation

$$(41)\qquad \sum X\frac{\partial x}{\partial u}+\frac{\partial r}{\partial u}+\frac{\partial \log \sqrt{E}}{\partial v}f'=0,$$

or, by (9),

$$(41')\qquad \sqrt{E}\frac{\partial \phi}{\partial v}+2\frac{\partial r}{\partial u}-\frac{\partial \sqrt{E}}{\partial v}\phi=0.$$

The elimination of r between this equation and (40) leads to an equation in ϕ of the third order. Hence the

THEOREM.—*The determination of all congruences whose principal ruled surfaces are represented by a given family of great circles and their orthogonal trajectories and correspond to the principal surfaces of the conjugate congruence requires the solution of a partial differential equation of the third order.*

The condition (41) is the same as that which expresses that C_1 is normal when C is normal. Since in the latter case the principal surfaces are developable we have the

THEOREM.—*When a congruence and the conjugate corresponding to one family of developables are both normal, their developable surfaces correspond.*

When C is a normal congruence the equation (40) reduces to

$$(42)\qquad \frac{\partial}{\partial u}\left(2\frac{\partial r}{\partial v}+\frac{\partial \log E}{\partial v}r\right)=0,$$

for which the general integral is

$$(43)\qquad r=\frac{1}{\sqrt{E}}\left(\int \sqrt{E}V du+U\right),$$

where U and V are functions of u and v respectively. From (9) we see that in the present case the coördinates of the mean surface of the congruence are given by

$$(43') \qquad \frac{\partial x}{\partial u} = -r\frac{\partial X}{\partial u} + \frac{\partial r}{\partial u}X, \qquad \frac{\partial x}{\partial v} = r\frac{\partial X}{\partial v} - \frac{1}{E}\frac{\partial (rE)}{\partial v}X.$$

Denoting by ρ the abscissa of one of the normal surfaces, we have

$$\frac{\partial \rho}{\partial u} = -\sum X\frac{\partial x}{\partial u}, \qquad \frac{\partial \rho}{\partial v} = -\sum X\frac{\partial x}{\partial v},$$

or, with the aid of equations (43′),

$$\frac{\partial \rho}{\partial u} = -\frac{\partial r}{\partial u}, \qquad \frac{\partial \rho}{\partial v} = \frac{\partial r}{\partial v} + \frac{\partial \log E}{\partial v}r.$$

By means of (43) we get from these equations

$$\rho = -r + 2\int V dv,$$

where V is the same function which appears in (43).

From (41′) and (42) it is seen that if C_1 is also to be a normal congruence we must have

$$\frac{\partial r}{\partial u} = 0, \qquad r\frac{\partial^2 \log E}{\partial u\,\partial v} = 0.$$

Excluding isotropic congruences, or, in other words, the case $r = 0$, we see that the necessary and sufficient conditions that C and C_1 be normal congruences is that r be a function of v alone and $\sqrt{E}$ be the product of a function of u and a function of v. If the latter condition is to be satisfied, either $U_1 = 0$, $U_2 = 0$, or $U_1 = \lambda U_2$, where λ is a constant; and conversely. Recalling our previous results, we see that for the first two cases the finding of the direction cosines is equivalent to the determination of a plane curve from its intrinsic equation and in the last case of a general helix from its intrinsic equations. Since both of these determinations require quadratures only, we have the

THEOREM.—*The complete determination of all normal congruences for which, when the ruled surfaces $u = const.$, $v = const.$ are the developables, the conjugate congruence also is normal, reduces to quadratures.*

§ 7. *When the system on the sphere is the image of the mean surfaces or of a family of developables.*

From (17) we see that the finding of all congruences for which one family of mean ruled surfaces is represented by a given family of great circles requires the determination of two functions r and ϕ satisfying the equation:

$$\frac{1}{\sqrt{E}}\frac{\partial^2 r}{\partial u^2}-\sqrt{E}\frac{\partial^2 r}{\partial v^2}+\frac{\partial}{\partial u}\frac{1}{\sqrt{E}}\frac{\partial r}{\partial u}-3\frac{\partial}{\partial v}\sqrt{E}-2\frac{\partial^2}{\partial v^2}\sqrt{E}\cdot r$$

(44)

$$=\frac{\partial}{\partial u}\left(\frac{1}{\sqrt{E}}\frac{\partial\phi}{\partial u}\right)+\frac{\partial}{\partial v_1}\left(\sqrt{E}\frac{\partial\phi}{\partial v}\right)+2\sqrt{E}\phi.$$

From (31) we see that the necessary and sufficient condition that the ruled surfaces $u=$ const., $v=$ const. of C_1 also be its mean ruled surfaces is

$$\sum X\frac{\partial x}{\partial v}+\frac{\partial r}{\partial v}=0,$$

or by (16)

$$\frac{\partial}{\partial u}(r-\phi)=0,$$

from which we have

(45) $$r=\phi+V,$$

where V is a function of v alone. Substituting this expression for r in (44) we have

$$\frac{\partial^2\phi}{\partial v^2}+\frac{\partial\log E}{\partial v}\frac{\partial\phi}{\partial v}+\left(\frac{1}{\sqrt{E}}\frac{\partial^2}{\partial v^2}\sqrt{E}+1\right)\phi$$

(46)

$$=-\tfrac{1}{2}\left[V''+3\frac{\partial\log\sqrt{E}}{\partial v}V'+2\frac{1}{\sqrt{E}}\frac{\partial^2\sqrt{E}}{\partial v^2}V\right],$$

where the accents denote differentiation with respect to v. From (45) and (46) we see that, when V is given an arbitrary form, the determination of r requires the solution of an ordinary differential equation of the second order. The expressions for the coördinates of one of the limit surfaces follow from (16).

When C is a normal congruence the above equation reduces to

$$V''+3\frac{\partial\log\sqrt{E}}{\partial v}V'+2\frac{1}{\sqrt{E}}\frac{\partial^2\sqrt{E}}{\partial v^2}V=0.$$

Hence E must be a function of v alone, and consequently

$$\sqrt{E}=a\cos v+b\sin v,$$

where a and b are constants. But this is a subcase of that characterized by the equation

$$U_1=\lambda U_2,$$

previously discussed; hence the direction-cosines X, Y, Z can be found by quadratures. When we put the above expression for $\sqrt{E}$ and $\phi=0$ in (44), it

reduces to a form from which r can be found by two quadratures. Thus, by (45),

$$r = V = \frac{k_1(a \sin v - b \cos v) + k_2}{(a \cos v + b \sin v)^2}.$$

where k_1 and k_2 are constants. Hence the

THEOREM.—*The complete determination of normal congruences whose mean ruled surfaces correspond to the mean ruled surfaces of the corresponding conjugate congruence reduces to quadratures.*

It is readily found that condition (32) is not satisfied, and therefore

The corresponding conjugate congruence is not a normal one.

Lastly, we consider the determination of congruences for which one system of developables has for its spherical representation the orthogonal trajectories of a given family of great circles. In this case equation (22) reduces to such a form that for any value of ϕ the finding of r requires two quadratures.

In order that the ruled surfaces $u = \text{const.}$ of the corresponding conjugate congruence C_1 be developable we must have* $f_1 = 0$ and hence by (31) $f = 0$. Consequently $f = f'$, so that C is a normal congruence, which is entirely in accord with the preceding results.

In order that the ruled surfaces $v = \text{const.}$ of C_1 be developables we must have by (31) and (21)

$$4\frac{\partial r}{\partial u} - \frac{\partial E}{\partial v}\phi = 0.$$

Eliminating r between this equation and the equation to which (22) reduces in this case, we find that ϕ satisfies a linear equation of the third order in the derivatives of ϕ with respect to u. Hence the

THEOREM.—*When the cosines X, Y, Z for a given system of great circles $u = \text{const.}$ and their orthogonal trajectories $v = \text{const.}$ are found, the determination of all congruences having these trajectories for the representation of one family of developables reduces to quadratures. Only when C is a normal congruence can the ruled surfaces $u = \text{const.}$ of the conjugate be developables. And the determination of all congruences for which the ruled surfaces $v = \text{const.}$ of the conjugate are developables requires the integration of an ordinary differential equation of the third order.*

PRINCETON, *October*, 1901.

* BIANCHI, l. c., p. 252.

CONSTRUCTIVE THEORY OF THE UNICURSAL CUBIC BY SYNTHETIC METHODS*

BY

D. N. LEHMER

1. SCHROETER'S† classic work on the general cubic leaves little to be desired in point of symmetry and generality. It is nevertheless interesting to build up the theory of the unicursal cubic, the curve being defined as the locus of the intersection of corresponding rays of two projective pencils, one of the first and the other of the second order. This has in fact been done by DRASCH.‡ The following discussion, based likewise on this definition, is materially simplified by the use of the properties of the point designated in § 7 by Σ. Incidentally the investigation brings to light a remarkable one-to-one correspondence between the points of the plane and the line elements on the cubic.

2. The locus described above has at least one and at most three points in common with any line in the plane. We assume the truth of this theorem, a proof of which may be found in the eleventh chapter of REYE'S *Geometrie der Lage*.

Notations.—Throughout this paper we shall use the following notations: The pencil of the first order will be denoted by s, its center by S, and its rays by a, b, c, etc. The pencil of the second order (and also the conic enveloped by it) will be denoted by κ, and the rays by α, β, γ, etc. The cubic itself will be denoted by C.

3. THEOREM.—*No point of the cubic C lies within the conic κ.*

4. THEOREM.—*The cubic C touches the conic κ in at least one point, and at most in three.*

To prove this take S', a point on κ, for the center of a pencil s' of the first order perspective to κ. This pencil generates with s a conic which cuts κ in at least one and at most three other points besides S'. These are easily seen to be points on C.

* Presented to the Society (San Francisco) May 3, 1902. Received for publication May 12, 1902.

† SCHROETER, *Die Theorie der ebenen Kurven dritter Ordnung*, Teubner, Leipzig, 1888. See also BINDER, *Theorie der unicursalen Plancurven vierter bis dritter Ordnung*, Teubner, Leipzig, 1896.

‡ DRASCH, *Beitrag zur synthetischen Theorie der ebenen Curven dritter Ordnung mit Doppelpunkt*, Wiener Berichte, vol. 85 (1882), p. 534.

5. THEOREM. *If S is outside of κ it is a double point of C. The rays of s which correspond to the tangents of κ through S are the principal tangents to C at S.*

The rays of κ through S meet their corresponding rays in that point. Every ray of s in this case meets C in three points; two at S, and one where it meets its corresponding ray of κ. These three points tend to coincide as the ray of κ approaches as a limiting position either tangent from κ through S.

6. THEOREM.—*If S is on κ it is a cusp of C.*

7. PROBLEM.—*Given S and κ with three pairs of corresponding rays, to construct C.*

Let the three given pairs be a, α; b, β; and c, γ. The intersection of a and α will be a point A on C. Draw through A the other tangent v to κ. Take this line perspective to κ. Draw through A any other line u. Take this perspective to s. The lines u and v are seen to be in perspective position. Their center of perspectivity may be found by joining any two pairs of corresponding points of u and v such as (v, β) with (u, b) and (v, γ) with (u, c). This center of perspectivity we shall denote by Σ. The importance of this point in the theory of the cubic depends upon the following theorem:

8. THEOREM.—*The locus of Σ as u revolves about A is a straight line a' passing through S. The point row Σ is projective to the pencil u.*

For as u revolves, (u, b) and (u, c) project to the fixed points (v, β) and (v, γ) in two projective pencils which generate the locus of Σ. These pencils are perspective since they have the corresponding ray v in common. The locus of Σ is thus a straight line. It passes through S as is seen by giving u the direction AS. The rest of the theorem is sufficiently evident.

9. THEOREM.—*The intersection of a' with v is a point A' on C.*

This is seen by drawing the ray of κ corresponding to a' (§ 8). It follows from this theorem that the line v meets the cubic in three real points. To find the third point A'' we must determine the ray of s corresponding to V. Let T be the point of tangency of V, and let (T, Σ) cut u in U. Then (U, S) meets v in A''.

10. THEOREM.—*The tangents from Σ to κ meet u in points on C.*

This important theorem is seen to be true by drawing the rays of s corresponding to these tangents.

11. PROBLEM.—*To find a line u through A corresponding to a given point Σ on a'.*

The required line passes through the intersection of c with the line joining Σ to (v, γ). It also passes through the intersection of b with the line joining Σ to (v, β). The solution of this problem furnishes a very expeditious method of constructing C by points. Construct for each point on a' the corresponding line u and get its intersections with C by the previous theorem. According as Σ lies within or without κ the line u will meet C in one or three points.

12. PROBLEM.—*To draw all the tangents from A to C.*

Take for Σ the points where a' meets κ. The line u by § 10 meets C in two coincident points. The points on u might also coalesce if Σ should fall upon u. In such a case Σ would lie on C, and would be either at S or A'. When Σ is at S the u line is AS which is not a true tangent. When Σ is at A', u coincides with v. One of the tangents from Σ to κ coincides with u and gives no definite intersection. The u line in this case is not a tangent to C, since A and A' are not in general coincident.

13. THEOREM.—*Two tangents or none may be drawn from A to C according as a' does or does not intersect κ.*

The case where a' is tangent to κ will be discussed later (§ 19).

14. THEOREM.—*If S lies outside of κ, two tangents or none may be drawn from any point on the cubic to the cubic. If S is inside κ, two such tangents may always be drawn. If S is on κ, one and only one such tangent may be drawn.*

This theorem follows from the fact (§ 8) that a' passes through S. In the third case one of the points where a' meets κ is at S, and does not give a true tangent (§ 12).

15. PROBLEM.—*To draw the tangent to C at A.*

Take for Σ the point where a' meets α. For in this case one of the tangents from Σ to κ meets u in A, so that u meets C in two coincident points at A.

16. THEOREM.—*Let the line u through $(a_1\alpha_1)$ meet C again in the points $(a_2\alpha_2)$ and $(a_3\alpha_3)$. Then as u revolves about $(a_1\alpha_1)$ the pencils a_2 and a_3 are in involution, as are also the pencils a_2' and a_3'.*

By the theorem of § 10, a_1' passes through (α_2, α_3). Also a_2' passes through (α_3, α_1) and a_3' through (α_1, α_2). As u revolves, (α_2, α_3) describes the fixed line a_1'. Therefore α_2 and α_3 are pairs of tangents to κ in involution. The corresponding rays a_2 and a_3 are therefore in involution. Further α_2 and α_3 cut out on α_1 two point rows in involution which project to S in the rays a_2' and a_3', which are therefore in involution.

Clearly if u is drawn tangent to C, the two rays a_2 and a_3 fall together and are thus a double ray in the involution. Again if C has a double point at S the principal tangents at S are also a pair of corresponding rays in the involution Now any pair of corresponding rays in an involution are harmonic conjugates with respect to the pair of double rays. From this follows easily the well-known theorem:

17. THEOREM.—*In a cubic with a double point S, if two rays be drawn through S harmonically conjugate to the principal tangents at S, these rays will meet the cubic in two points such that the tangents at those points will meet again on the cubic.*

18. THEOREM.—*The rays a and a' are corresponding rays of a pencil in involution.*

Using the notation of § 16 we see that α_2 cuts out on α_1 a point row projective to a_2 and perspective to a_3', and therefore projective to a_2' by § 16. The pencil a_2 is therefore projective to the pencil a_2'. We have also on the line v, A, A'; (v, b), (v, γ); (v, c), (v, β), three pairs of points in involution, being the section by v of the complete four point, S, Σ, (u, b), (u, c). By projecting to S we have a and a' corresponding to each other doubly.

19. PROBLEM.—*Given a line a' through S to find the corresponding point A on C.*

By the preceding theorem we derive the line a from a' in the same way in which we derive a' from a (§ 7). In the case of a cubic with a double point we may ask what is the line a' corresponding to one of the principal tangents at S. It is not difficult to see that the corresponding line is one of the tangents from S to κ. Referring to § 13 we have

20. THEOREM.—*A cubic is divided by its double point into two portions such that from a point in one portion two tangents may be drawn to the cubic, while from a point in the other portion no such tangent may be drawn.*

21. THEOREM.—*To every point in the plane there corresponds a point on C, with a direction through that point and conversely.*

Let the point be Σ. Join it to S. Call this line a' and by § 19 get the corresponding point A. To the point Σ on a' corresponds a definite line u, through A. An apparent exception exists for two points Σ which lie one on one tangent from S to κ and one on the other. The corresponding point on C is S for either point. The point S for one point Σ is to be considered as belonging to one branch of the curve; and for the other point Σ as belonging to the other branch.

22. THEOREM.—*The locus of points Σ which give tangents to C from the corresponding points on C, is the conic κ.*

This follows from § 12.

23. THEOREM.—*The locus of points Σ which give tangents to C at the corresponding points, is a point row C' of the third order, having the same base conic κ and the same center S for its pencil of the first order.*

For Σ thus defined is the locus of the intersection of a' with α by § 15. But by the discussion of § 18 it is seen that these are projective pencils, one of the first and one of the second order.

24. THEOREM.—*There are at most three points of inflection on C, and at least one.*

For the cubic C' of the preceding paragraph touches κ in at least one point and at most in three. These points correspond to inflection points on C, because one tangent *from* the point on C, coincides with the tangent *at* the point.

25. THEOREM.—*If S is outside of κ, the "tangential cubic" C', defined above, has for its principal tangents the tangents from S to κ.*

To find the principal tangents T_1 and T_2 to the cubic C, we found the rays of s corresponding to the rays τ_1 and τ_2 of κ which pass through S (§ 5). We must then find for the cubic C' the Σ lines corresponding to T_1 and T_2, which by § 19 are t_1, and t_2, the rays of s tangent to κ.

26. This last theorem, which was noted by one of my students, MR. B. O. LACEY, may be made the basis of a proof that the cubic with real double point has only one real inflection. Other theorems may be obtained without difficulty, but the power of the method has already been sufficiently indicated.

BERKELEY, CALIFORNIA,
January, 1901.

THE GROUPS OF STEINER IN PROBLEMS OF CONTACT

(SECOND PAPER)*

BY

LEONARD EUGENE DICKSON

1. Denote by G the group of the equation upon which depends the determination of the curves of order $n-3$ having simple contact at $\frac{1}{2}n(n-3)$ points with a given curve C_n of order n having no double points. The case in which n is odd was discussed in the former paper (Transactions, January, 1902) and G was shown to be a subgroup of the group defined by the invariants $\phi_3, \phi_4, \phi_5, \cdots$, the latter group being holoedrically isomorphic with the first hypoabelian group on $2p$ indices with coefficients taken modulo 2. For n even, G is contained in the group H defined by the invariants $\phi_4, \phi_6, \cdots$, with even subscripts. JORDAN has shown (*Traité*, pp. 229–242) that H is holoedrically isomorphic with the abelian linear group A on $2p$ indices with coefficients taken modulo 2. The object of the present paper is to establish the latter theorem by a short, elementary proof, which makes no use of the abstract substitutions $[\alpha_1, \beta_1, \cdots, \alpha_p, \beta_p]$ of JORDAN, and which exhibits explicitly the correspondence† between the substitutions of the isomorphic groups.

2. We first define a non-homogeneous linear group A_1 on $2p$ indices which leaves the function $x_1y_1 + \cdots + x_py_p$ invariant modulo 2 and which is holoedrically isomorphic with the abelian group A. To the generators M_i, L_i, N_{ij} of A we make correspond the respective substitutions of A_1:

$$\mu_i: \quad x_i' = y_i, \quad y_i' = x_i;$$

$$\lambda_i: \quad x_i' = x_i + y_i + 1;$$

$$\nu_{ij}: \quad x_i' = x_i + y_j, \quad x_j' = x_j + y_i.$$

Then to the general substitution of A,

$$S: \quad x_i' = \sum_{j=1}^{p}(\alpha_{ij}x_j + \gamma_{ij}y_j), \quad y_i' = \sum_{j=1}^{p}(\beta_{ij}x_j + \delta_{ij}y_j) \quad (i = 1, \cdots, p),$$

will correspond the following substitution of A_1:

* Presented to the Society February 22, 1902. Received for publication January 13, 1902.

† It is shown in § 6 that this correspondence is in accord with that given by JORDAN.

$$\sigma: \quad \begin{aligned} x_i' &= \sum_{j=1}^{p}(\alpha_{ij}x_j + \gamma_{ij}y_j) + \sum_{j=1}^{p}\alpha_{ij}\gamma_{ij}, \\ y_i' &= \sum_{j=1}^{p}(\beta_{ij}x_j + \delta_{ij}y_j) + \sum_{j=1}^{p}\beta_{ij}\delta_{ij} \end{aligned} \qquad (i=1,\cdots,p).$$

In fact, the general correspondence $S \sim \sigma$ includes the assumed correspondences

$$M_i \sim \mu_i, \qquad L_i \sim \lambda_i, \qquad N_{ij} \sim \nu_{ij} \qquad (i,j=1,\cdots,p).$$

Moreover, if $S_1 \sim \sigma_1$, it is readily verified that

$$M_iS_1 \sim \mu_i\sigma_1, \qquad L_iS_1 \sim \lambda_i\sigma_1, \qquad N_{ij}S_1 \sim \nu_{ij}\sigma_1 \quad (i,j=1,\cdots,p).$$

Since the generators $\mu_i, \lambda_i, \nu_{ij}$ leave invariant the function $x_1y_1 + \cdots + x_py_p$, the general substitution σ of the group A_1 will leave it invariant.

3. THEOREM.*—*The group A_1 may be represented as a doubly transitive substitution group on the $R_p \equiv 2^{2p-1} - 2^{p-1}$ letters $(x_1y_1x_2y_2\cdots x_py_p)$ in which $x_1, y_1, \cdots x_p, y_p$ assume every system of solutions, not all zero, of the congruence*

$$x_1y_1 + x_2y_2 + \cdots + x_py_p \equiv 1 \pmod 2. \tag{1}$$

That A_1 is transitive on the R_p letters may be shown by the usual methods of linear group theory, or directly by the following remark. Let $(\alpha_1\gamma_1\cdots\alpha_p\gamma_p)$ be an arbitrary one of the letters. Then $\alpha_1\gamma_1 + \cdots + \alpha_p\gamma_p \equiv 1 \pmod 2$. One substitution which belongs to A_1 and which replaces $(11\,00\cdots00)$ by $(\alpha_1\gamma_1\cdots\alpha_p\gamma_p)$ is the following:

$$\begin{aligned} x_1' &= (\alpha_1\gamma_1 + \alpha_1 + \gamma_1)x_1 + (\alpha_1+1)y_1 + \sum_{i=2}^{p}\{(\alpha_1+1)\gamma_ix_i + (\alpha_1+1)\alpha_iy_i\} \\ &\qquad + (\alpha_1+1)(\gamma_1+1), \\ y_1' &= (\gamma_1+1)x_1 + (\alpha_1\gamma_1 + \alpha_1 + \gamma_1)y_1 + \sum_{i=2}^{p}\{(\gamma_1+1)\gamma_ix_i + (\gamma_1+1)\alpha_iy_i\} \\ &\qquad + (\alpha_1+1)(\gamma_1+1), \\ x_j' &= \alpha_j(\gamma_1+1)x_1 + \alpha_j(\alpha_1+1)y_1 + (\alpha_j\gamma_j+1)x_j + \alpha_jy_j \\ &\qquad + \sum{}'(\alpha_j\gamma_ix_i + \alpha_j\alpha_iy_i) + \alpha_j(\alpha_1+\gamma_1+1), \\ y_j' &= \gamma_j(\gamma_1+1)x_1 + \gamma_j(\alpha_1+1)y_1 + \gamma_jx_j + (\alpha_j\gamma_j+1)y_j \\ &\qquad + \sum{}'(\gamma_j\gamma_ix_i + \gamma_j\alpha_iy_i) + \gamma_j(\alpha_1+\gamma_1+1), \end{aligned}$$

where $\sum'$ denotes the summation $i = 2, \cdots, p;\ i \neq j$.

* For other applications one might employ the theorem that the group A_1 permutes transitively the 2^{2p} functions $a_1x_1 + b_1y_1 + \cdots + a_px_p + b_py_p + a_1b_1 + \cdots + a_pb_p$.

To prove that the group is doubly transitive, it now suffices to show that the subgroup leaving the letter (11 00 $\cdots$ 00) fixed is transitive on the remaining letters. The conditions that the general substitution σ of A_1 shall leave fixed the letter (11 00 $\cdots$ 00) are*

$$\alpha_{i1} + \gamma_{i1} + \sum_{j=1}^{p} \alpha_{ij}\gamma_{ij} \equiv \epsilon_{i1}, \qquad \beta_{i1} + \delta_{i1} + \sum_{j=1}^{p} \beta_{ij}\delta_{ij} \equiv \epsilon_{i1} \quad (i=1,\cdots,p).$$

With these conditions satisfied, S belongs† to the second hypoabelian group (with x_1 and y_1 playing the special rôle). Employing these conditions, we may give to σ the form:

$$x'_i = \sum_{j=1}^{p} (\alpha_{ij}x_j + \gamma_{ij}y_j) + \alpha_{i1} + \gamma_{i1} + \epsilon_{i1},$$
$$y'_i = \sum_{j=1}^{p} (\beta_{ij}x_j + \delta_{ij}y_j) + \beta_{i1} + \delta_{i1} + \epsilon_{i1} \qquad (i=1,\cdots,p).$$

It replaces (11 10 $\cdots$ 00) by $(a_1c_1\ a_2c_2 \cdots a_pc_p)$, where

$$a_1c_1 + \cdots + a_pc_p \equiv 1 \pmod 2,$$

if

$$\alpha_{i2} + \epsilon_{i1} = a_i, \qquad \beta_{i2} + \epsilon_{i1} = c_i \qquad (i=1,\cdots,p). \tag{2}$$

To show that the second hypoabelian group contains a substitution S whose coefficients satisfy the conditions (2), we note that the inverse S^{-1} is obtained by replacing α_{ij}, β_{ij}, γ_{ij}, δ_{ij} by δ_{ji}, β_{ji}, γ_{ji}, α_{ji}, respectively, so that the conditions (2) give the following conditions on S^{-1}:

$$\delta_{2i} \equiv a_i + \epsilon_{i1}, \qquad \beta_{2i} \equiv c_i + \epsilon_{i1} \pmod 2 \qquad (i=1,\cdots,p).$$

Hence the coefficients of y'_2 in S^{-1} are fully determined. Also

$$\beta_{21} + \delta_{21} + \sum_{i=1}^{p} \beta_{2i}\delta_{2i} \equiv a_1 + c_1 + (a_1+1)(c_1+1) + \sum_{i=2}^{p} a_ic_i$$
$$\equiv \sum_{i=1}^{p} a_ic_i + 1 \equiv 0 \pmod 2.$$

But‡ the second hypoabelian group contains such a substitution S^{-1}.

4. THEOREM.—*The groups H and A_1 are identical.*

It is first shown that every substitution of A_1 belongs to H. By § 4 of the former paper, μ_i and ν_{ij} (which have the same form as M_i and N_{ij}, respectively)

* Henceforth ϵ_{ij} denotes 1 if $i=j$, but denotes 0 if $i \neq j$.

† Bulletin of the American Mathematical Society, vol. 4 (1898), p. 504.

‡ DICKSON, *Linear Groups*, p. 202; or, American Journal of Mathematics, vol. 21 (1899), p. 227.

leave the functions $\phi_3, \phi_4, \phi_5, \cdots$ invariant. Next, λ_1 replaces the general term of ϕ_4 by

$$(x_1' + y_1' + 1 \;\; y_1' \cdots)(x_1'' + y_1'' + 1 \;\; y_1'' \cdots)(x_1''' + y_1''' + 1 \;\; y_1''' \cdots)$$
$$(x_1' + x_1'' + x_1''' + y_1' + y_1'' + y_1''' + 1 \;\; y_1' + y_1'' + y_1''' \cdots),$$

which is seen to be a term of ϕ_4. In like manner, it may be shown that λ_1 leaves invariant $\phi_6, \phi_8, \cdots$; but alters $\phi_3, \phi_5, \cdots$.

It is next shown that every substitution of H belongs to A_1. Let L be an arbitrary substitution of H and let it replace the letters

$$l_1 \equiv (00 \;\; 11 \;\; 00 \;\; \cdots \;\; 00), \quad l_2 \equiv (10 \;\; 11 \;\; 00 \;\; \cdots \;\; 00)$$

by certain letters l_1', l_2', respectively. By § 3, A_1 contains a substitution L' which replaces l_1 by l_1' and l_2 by l_2'. Hence $M \equiv L'^{-1} L$ will belong to H and will leave fixed the letters l_1, l_2. Since M does not alter ϕ_4, it will leave invariant the sum ψ of those terms of ϕ_4 which contain the factor $l_1 l_2$. The general term of ψ is therefore

$$l_1 l_2 (x_1 y_1 \;\; x_2 y_2 \;\; x_3 y_3 \cdots)(x_1 + 1 \;\; y_1 \;\; x_2 y_2 \;\; x_3 y_3 \cdots).$$

In view of (1), the last two expressions denote letters if, and only if,

$$\sum_{i=1}^{p} x_i y_i \equiv 1, \qquad y_1 \equiv 0 \pmod 2.$$

But the letters l_1 and l_2 satisfy these congruences. Hence ψ involves exactly $2R_{p-1}$ letters. Hence M must permute amongst themselves the remaining $R_p - 2R_{p-1} \equiv 2^{2p-2}$ letters, the general one of which is

$$(3) \qquad (x_1 \;\; 1 \;\; x_2 y_2 \;\; x_3 y_3 \cdots), \qquad x_1 + \sum_{i=2}^{p} x_i y_i \equiv 1 \pmod 2.$$

The substitutions of A_1 which leave unaltered the letters l_1 and l_2 permute transitively the 2^{2p-2} letters (3).

Indeed, by § 3, the substitutions of A_1 which leave l_1 fixed have the form

$$x_i' = \sum_{j=1}^{p} (\alpha_{ij} x_j + \gamma_{ij} y_j) + \alpha_{i2} + \gamma_{i2} + \epsilon_{i2},$$
$$y_i' = \sum_{j=1}^{p} (\beta_{ij} x_j + \delta_{ij} y_j) + \beta_{i2} + \delta_{i2} + \epsilon_{i2} \qquad (i = 1, \cdots, p).$$

The latter leaves l_2 fixed if, and only if,

$$\alpha_{11} = 1, \quad \alpha_{21} = 0, \quad \beta_{11} = 0, \quad \beta_{21} = 0, \quad \alpha_{i1} = \beta_{i1} = 0 \qquad (i = 3, \cdots, p).$$

Let σ_1 denote the general substitution so defined and let S_1 denote the corresponding homogeneous substitution. Let $(c_1 1\ c_2 d_2\ c_3 d_3 \cdots)$ be an arbitrary lette ˙ the form (3). The conditions that σ_1 shall replace $(01\ 11\ 00 \cdots 00)$ by $(c_1\ \ c_2 d_2 \cdots)$ are

$$(4)\quad c_1 = \gamma_{11},\ 1 = \delta_{11},\ c_2 = \gamma_{21} + 1,\ d_2 = \delta_{21} + 1,\ c_i = \gamma_{i1},\ d_i = \delta_{i1}\ \ (i = 3, \cdots, p).$$

To prove that there exists a substitution σ_1 satisfying the conditions (4) we follow the method used at the end of § 3. We observe that S_1^{-1} is the most general substitution of the second hypoabelian group (with x_2, y_2 playing the special rôle) which leaves the index y_1 unaltered. The conditions (4) give the following conditions modulo 2 on S_1^{-1}

$$\alpha_{11} \equiv 1,\ \gamma_{11} \equiv c_1,\ \alpha_{12} \equiv d_2 + 1,\ \gamma_{12} \equiv c_2 + 1,\ \alpha_{1i} \equiv d_i,\ \gamma_{1i} \equiv c_i\ \ (i = 3, \cdots, p).$$

Hence the coefficients of x_1' in S_1^{-1} are fully determined. Also, by (3),

$$\alpha_{12} + \gamma_{12} + \sum_{i=1}^{p} \alpha_{1i}\gamma_{1i} \equiv 1 + c_1 + \sum_{i=2}^{p} c_i d_i \equiv 0 \pmod 2.$$

But the second hypoabelian group contains a substitution of the form

$$y_1' = y_1,\quad x_1' = \sum_{i=1}^{p} (\alpha_{1i}x_i + \gamma_{1i}y_i),\ \cdots,\quad (\alpha_{12} + \gamma_{12} + \sum_{i=1}^{p} \alpha_{1i}\gamma_{1i} \equiv 0,\ \alpha_{11} \equiv 1).$$

Next, let M replace $l_3 \equiv (01\ 11\ 00 \cdots 00)$ by a letter l_3' of the form (3). By the preceding result, A_1 contains a substitution T which replaces l_3 by l_3'. Hence $M = TQ$, where Q is a substitution of H which leaves fixed the letters l_1, l_2, l_3. By § 9 of the former paper, Q permutes amongst themselves the R_{p-1} letters $(00\ x_2y_2\ x_3y_3 \cdots)$. The theorem may now be established by induction from $p-1$ to p. We proceed as in § 10 of the earlier paper,* deleting the functions ϕ_3 and $\phi_3^{(p-1)}$. As a basis for the induction, we show that the theorem is true for $p = 2$, whence $R_p = 6$. The six letters

$$(0011),\quad (1011),\quad (0111),\quad (1100),\quad (1101),\quad (1110),$$

cannot be combined to give a term of ϕ_4, so that the latter does not exist when $p = 2$. Evidently ϕ_6 is the product of the six letters. Hence H is the symmetric group on six letters. But the order of the quaternary abelian group modulo 2 is $(2^4 - 1)2^3(2^2 - 1)2 \equiv 6!$ Hence the groups H and A_1 are identical when $p = 2$†.

*One part of the proof by induction was there omitted, viz., the proof for the case $p = 2$, whence $R_2 = 6$. That G_1 and Γ are identical follows from the equality of their orders (see § 11), or more simply since Q is, for $p = 2$, either the identity or else is M_2, permuting (1101) with (1110), and hence is hypoabelian

† For a direct proof of the holoedric isomorphism of the symmetric group on 6 letters and the quaternary abelian group modulo 2, see *Linear Groups*, p. 99.

5. It follows that the order w_p of H satisfies the recursion formula

$$w_p = R_p(R_p - 1)2^{2p-2} \cdot \frac{w_{p-1}}{R_{p-1}} \equiv (2^{2p} - 1)2^{2p-1} \cdot w_{p-1}.$$

Since $w_2 = (2^4 - 1)2^3(2^2 - 1)2$, we derive the result,

$$w_p = (2^{2p} - 1)2^{2p-1}(2^{2p-2} - 1)2^{2p-3} \cdots (2^2 - 1)2.$$

6. To show that the above correspondence of operators of the isomorphic groups H and A is in accord with that obtained by JORDAN, we note that, in view of p. 241 of *Traité des substitutions*,

$$[11\ 00 \cdots 00] \sim M_1, \quad [10\ 00 \cdots 00] \sim L_1, \quad [10\ 10\ 00 \cdots 00] \sim L_2 L_1 N_{12}.$$

Also (*Traité*, p. 230), $[11\ 00 \cdots]$ leaves $(x_1 y_1\ x_2 y_2 \cdots)$ fixed if $x_1 + y_1 \equiv 0 \pmod 2$, but replaces it by $(x_1 + 1\ y_1 + 1\ x_2 y_2 \cdots)$ if $x_1 + y_1 \equiv 1$, and hence may be designated

$$\mu_1: \quad x_1' = y_1, \ y_1' = x_1.$$

Likewise, $[10\ 00 \cdots]$ leaves $(x_1 y_1\ x_2 y_2 \cdots)$ fixed if $y_1 \equiv 1$, but replaces it by $(x_1 + 1\ y_1\ x_2 y_2 \cdots)$ if $y_1 \equiv 0$, and hence may be designated

$$\lambda_1: \quad x_1' = x_1 + y_1 + 1.$$

Next, $[10\ 10\ 00 \cdots]$ leaves $(x_1 y_1\ x_2 y_2 \cdots)$ fixed if $y_1 + y_2 \equiv 1$, but replaces it by $(x_1 + 1\ y_1\ x_2 + 1\ y_2\ x_3 y_3 \cdots)$ if $y_1 + y_2 \equiv 0$, and hence may be designated

$$\lambda_2 \lambda_1 \nu_{12}: \quad x_1' = x_1 + y_1 + y_2 + 1, \ x_2' = x_2 + y_1 + y_2 + 1.$$

It follows that $N_{12} \sim \nu_{12}$. In view of the symmetry, $N_{ij} \sim \nu_{ij}$, etc.

THE UNIVERSITY OF CHICAGO, *January* 10, 1902.